TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

PETTERI VISTIAHO

MARITIME CYBER SECURITY INCIDENT DATA REPORTING FOR AUTONOMOUS SHIPS

Master of Science Thesis

Examiners:
Marko Helenius
Bilhanan Silverajan

Examiners and topic approved on
1 November 2017

ABSTRACT

PETTERI VISTIAHO: Maritime Cyber Security Incident Data Reporting for Autonomous Ships
Tampere University of Technology
Master of Science Thesis, 51 pages, 8 Appendix pages
March 2018
Master's Degree Program in Information Technology
Major: Communication Systems and Networks
Examiner: Marko Helenius, Bilhanan Silverajan

Keywords: autonomous shipping, cyber security, data modeling, IODEF, incident reporting

The main research objective of this thesis was to find a suitable data model to be used for incident reporting purposes in the use case of autonomous shipping. To reach this objective, some research into the maritime industry, autonomous shipping, and incident management and reporting was needed. Research into these topics was conducted via a literature review.

After these topics were investigated, some current incident data modeling and sharing methods were researched. Out of these IODEF seemed like the most suitable one for our use case, so it was chosen for further inspection. The IODEF specification was looked into more closely and a conclusion was ultimately made that the IODEF data model is suitable for reporting incident data from autonomous ships to the shore control center. However, the model was still missing some key information needed for this use case, so an extension for the data model was designed.

The data model and extension were then put to test via different use scenarios to test applicability for the needs of autonomous shipping. From these use scenarios it was inferred that the model is applicable for the many different incident data reporting needs of autonomous shipping. Further analysis and testing was then conducted, including a transport test over cellular and satellite connections. The test and analysis further validated the use of the data model.

All in all, the research was a success and a good data model was found for reporting incidents from autonomous ships. The work with the data model will continue further outside this thesis.

TIIVISTELMÄ

PETTERI VISTIAHO: Maritime Cyber Security Incident Data Reporting for Autonomous Ships
Tampereen teknillinen yliopisto
Diplomityö, 51 sivua, 8 liitesivua
Maaliskuu 2018
Tietotekniikan diplomi-insinöörin tutkinto-ohjelma
Pääaine: Tietoliikennetekniikka
Tarkastajat: Marko Helenius, Bilhanan Silverajan

Avainsanat: autonominen laivankuljetus, IODEF, kyberturvallisuus, ongelmatapauksen raportointi, tiedon mallintaminen

Tämän diplomityön tärkein tutkimustavoite oli löytää sopiva datamalli käytettäväksi ongelmatapausten raportoimiseksi autonomisen laivankuljetuksen tapauksessa. Tähän tavoitteeseen pääsemiseksi tarvittiin tutkimusta aiheista kuten merenkulkuteollisuus, autonominen laivankuljetus ja ongelmatapausten hallinta ja raportointi. Näitä aiheita tutkittiin kirjallisuuskatsauksen keinoin.

Kun näihin aiheisiin oltiin tutustuttu, alettiin tutkia nykyisin käytössä olevia ongelmatapausten datan mallinnus- ja jakamismenetelmiä. Näistä IODEF vaikutti heti sopivimmalta työn käyttötapaukseen ja se valittiin tarkemmin tutkittavaksi. IODEF:n spesifikaatiodokumentteihin tutustuttiin tarkemmin ja päädyttiin siihen tulokseen, että IODEF:n datamalli on sopiva käytettäväksi ongelmatapausten datan raportointiin autonomiselta laivalta rannalla sijaitsevaan hallintakeskukseen. Datamallista puuttui kuitenkin vielä joitain tämän käyttötapauksen vaatimia tärkeitä tietoja, joten datamallille suunniteltiin laajennus.

Tämän jälkeen datamalli ja siihen suunniteltu laajennus pääsivät testattaviksi erilaisissa käyttöskenaarioissa, jotta mallin soveltuvuutta autonomisen laivankuljetuksen tarpeisiin voitiin testata. Näistä käyttöskenaariotesteistä saatiin selville, että tämä datamalli pystyy täyttämään autonomisen laivankuljetuksen monet erilaiset ongelmatapausten datan raportointitarpeet. Tämän jälkeen mallille suoritettiin lisäanalyysia ja -testausta, muun muassa siirtotestit matkapuhelinverkon ja satelliittiyhteyden tapauksissa. Tämä analyysi ja testit vahvistivat edelleen uskoa datamallin sopivuudesta tähän käyttötarkoitukseen.

Kaiken kaikkiaan tämä tutkimus onnistui erittäin hyvin ja hyvä datamalli ongelmatapausten raportoimiseksi autonomisilta laivoita löydettiin. Työtä tämän datamallin kanssa tullaan jatkamaan myös tämän diplomityön ulkopuolella.

PREFACE

The journey of writing my master's thesis was not without problems. I actually had to change the whole topic of my thesis after 3 months of preparations with the original topic. This ended up being a blessing in disguise, as I much prefer this topic over my original one. Problems aside, this journey has taught me a lot and I have been privileged to meet some awesome people along the way.

First and foremost, I would like to thank Bilhanan Silverajan for providing me with this awesome topic, being a huge help with the thesis, and providing me with a work opportunity at TUT as a research assistant. I would also like to thank Marko Helenius for being the main examiner of the thesis and being there for the thesis meetings. Joona Kannisto deserves a mention as he was also there for the thesis meetings and provided me with frequent access to one-on-one meetings to talk about my progress. A big thank you to Antti Kolehmainen for helping me setting up the transport tests at the later parts of the thesis. Lastly, I would like to thank my parents for always supporting me and believing in me throughout my whole university studies, even though it has not always been smooth sailing for me.

This thesis was done as a part of the DIMECC Design for Value (D4V) research program and in collaboration with NICT Japan.

Tampere, 12.3.2018

Petteri Vistiaho

CONTENTS

LISTS OF FIGURES AND TABLES

TERMS AND ABBREVIATIONS

AIS	Automatic Identification System
CSIRT	Computer Security Incident Response Team
ENISA	European Network and Information Security Agency
ETA	Estimated Time of Arrival
GPS	Global Positioning System
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IMO	International Maritime Organization
IODEF	Incident Object Description Exchange Format
ISO	International Organization for Standardization
JSON	JavaScript Object Notation
LIDAR	Light Detection and Ranging
MILE	Managed Incident Lightweight Exchange
MUNIN	Maritime Unmanned Navigation through Intelligence in Networks
NIST	National Institute of Standards and Technology
NMEA	National Marine Electronics Association
RFC	Request for Comments
RID	Real-time Inter-network Defense
ROLIE	Resource-Oriented Lightweight Information Exchange
SFTP	SSH File Transfer Protocol
STIX	Structured Threat Information eXpression
TAXII	Trusted Automated eXchange of Intelligence Information
TCP	Transmission Control Protocol
TUT	Tampere University of Technology
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VDR	Voyage Data Recorder
XML	eXtensible Markup Language

Autonomous shipping	The act of transporting cargo overseas via an autonomous vessel. The autonomous shipping chain includes ground transport to the ports, cargo handling at ports as well as transport overseas. The goal of autonomous shipping is to minimize the human input required to ship items.
Autonomous vessel	A ship that is unmanned and mostly self-navigating. It receives major navigation decisions through a satellite data link from a crew ashore if needed but can do navigational decisions itself by analyzing sensor and GPS data in a normal situation.
Cyber security	Protection of computer hardware and software assets, and data. It also aims to prevent any disruptions to the services these systems provide.
Incident data reporting	The act of reporting incident related data to the organization's CSIRT so that the incident can be resolved.

Incident data sharing	The act of sharing incident related data between organizations to improve cyber security.
Incident response	A term that describes the way an organization handles the aftermath of a security breach or cyberattack. The goal of incident response is to minimize the damage and downtime of the affected systems as well as to keep the costs caused by the incident at a minimum. Having a clear incident response plan helps organizations deal with incidents.
Maritime cyber security	A relatively new branch of cyber security that focuses on preventing cyberattacks targeted at the systems aboard vessels and the maritime control systems.
Security incident	An event that disrupts normal operations. It may indicate that an organization's network, system or data have been compromised or that a protective measure set in place to protect these has failed.
Security threat	A potential cause of an incident that might exploit a vulnerability to breach security and cause harm to systems and organizations.
Vulnerability	A weakness or flaw in the design, implementation or operation of a system that an attacker can exploit to reduce the system's information assurance.

1. INTRODUCTION

The maritime industry will be facing a huge change in the coming years as autonomous vessels become more commonplace. It is expected that fully autonomous ships, tugs, and ferries will be in use in some capacity by the year 2025. The first autonomous vessels will operate in small restricted areas, like ports or rivers, and later we will see autonomous ships on the open sea as well. [1]

An autonomous vessel is a ship that is usually unmanned and mostly self-navigating. It receives major navigational decisions through a satellite data link from a crew ashore, if needed, but can also make navigational decisions by itself by analyzing sensor and Global Positioning System (GPS) data in a normal situation. These vessels will be used for all kinds of tasks, including cargo shipping, ferrying cars and people across rivers, and tugging larger ships in harbors.

The use of autonomous ships will reduce the need for on-board crews, but it will create jobs on shore as people are needed to monitor and operate the vessels from control centers. These kinds of jobs are considerably more attractive for the young population than being stuck at sea for months at a time. Autonomous vessels are not going to remove the need for seafaring experts, they are just going to move the jobs to a more convenient location.

Most of the technology needed to build and operate these vessels is already there. Technologies related to autonomous ships are being tested in a designated test area in Norway right now [2]. A globally available test area for autonomous vessels, named Jaakonmeri Test Area, will be opened in late 2017 on the west coast of Finland [3]. There companies will be able to test their technologies related to autonomous maritime trafficking in open sea conditions, as well as icy conditions during the winter. For now, it is only possible to operate autonomous vessels inside the designated test areas, because of regulatory and legal problems.

The first autonomous cargo ship in the world is expected to be the Norwegian YARA Birkeland [2]. This ship is expected to start operating as a manned vessel by the year 2018, start remote operation in 2019 and then shift to fully autonomous operations in 2020. Remote controlled vessels are operated from the shore via a satellite link, whereas automated ships are automatically operated by technology [4]. Autonomous vessels are a mix between these two. The differences between these ship operating schemes are shown in Figure 1.

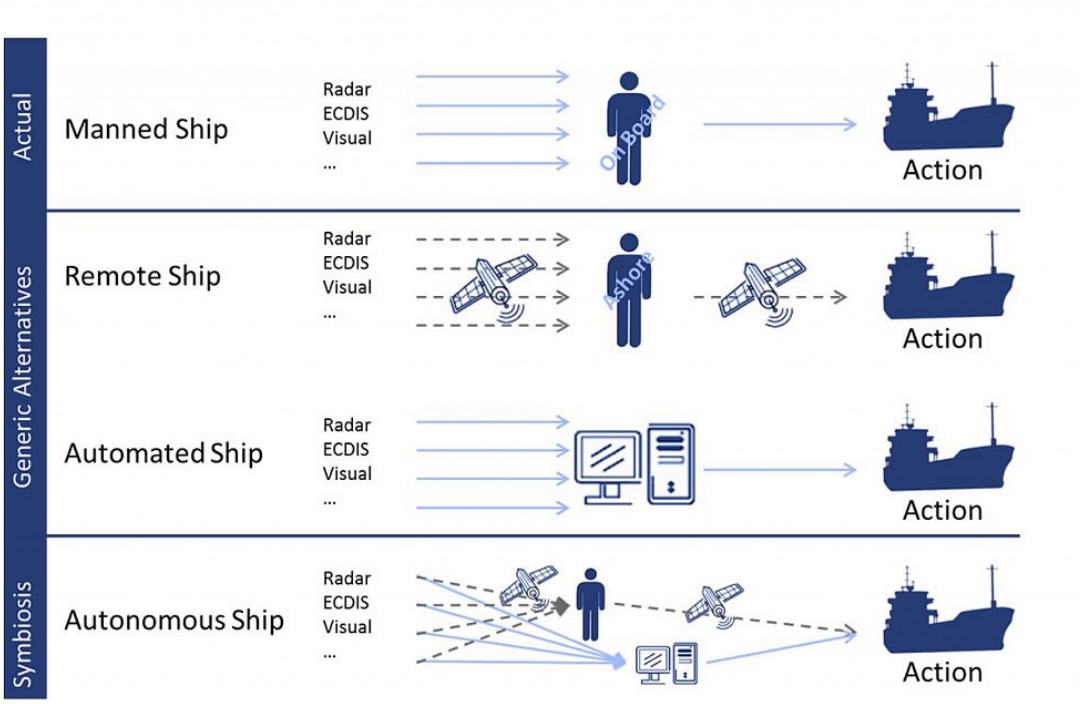

Figure 1. *Different ship operation schemes. [4]*

The introduction of autonomous ships will bring challenges for maritime cyber security as the satellite data links will be used more frequently and for more essential tasks than ever before. All kinds of data and instructions will be flowing back and forth through the satellite data link. This connection needs to be secured somehow, and what if something goes wrong? If a cyber security incident, or even a physical security one, is detected, what actions need to be taken and what kind of messages need to be sent and where?

Autonomous vessels can face all kinds of security threats at sea and at port. Cyber security threats include hacking into any of the equipment of the ship or the data link, GPS spoofing, malware, and many more. Physical security threats can include extremist or state-sponsored attacks towards the vessel, theft of cargo, and piracy. Cyber and physical security threats often go hand-in-hand as cyber threats can be used to gain physical access to the vessel or its cargo.

It is common practice to do predetermined actions when something goes wrong, this is called incident management. As autonomous shipping is a totally new area, it does not have common incident management and reporting practices set in place just yet. Therefore, it is important to research into these areas and come up with new industry standards for managing and reporting incidents regarding autonomous shipping.

Especially incident reporting faces new challenges with autonomous shipping. Firstly, it is hard to know if an incident has really happened or if we have a false positive, as no one is on board the ship. Secondly, the connectivity at sea can be problematic at times

and will make incident reporting harder. Lastly, knowing the information we need for a report and who to send the report to is not as straightforward as in traditional cases.

This thesis describes a data reporting model for cases when a security incident has been detected onboard an autonomous ship. The model describes the information that needs to be sent and the structure for the information. It is also explored where these messages need to be sent and what additional measures need to be taken when an incident has been detected.

1.1 Research Questions

This thesis has four distinct research questions:

1. What is the current state of autonomous shipping?
2. What is the current state of maritime physical and cyber security?
3. What are the common practices of incident management and reporting, and what kind of reporting methods are used currently?
4. What kind of a cyber security incident data reporting model would be the best for autonomous ships?

The fourth research question is the most important for the thesis. The rest of the questions need to be answered for background information and a basis on which a good answer for question 4 can be built upon.

1.2 Scope

The scope for research question 1 is set to explaining what autonomous shipping is and what challenges it may face in the future. Some current autonomous shipping concepts are also looked at and compared.

The scope for research question 2 is set to cover the current state and practices of maritime cyber and physical security as well as some security concerns directly related to autonomous shipping. The focus is on cyber security, and physical security is mainly just there as a side note.

The scope for research question 3 is set to shortly explaining the common practices of incident management and reporting and to introducing some currently used incident reporting methods. The focus is on the beginning of the incident management chain, from incident discovery, data collection, and incident reporting, to incident validation.

The scope for the incident data reporting model is set to include cases of cyber security incidents happening on a single autonomous ship, not a fleet of ships for example. The model focuses on transporting data between the ship and the command center. This doesn’t, however, mean that other uses for the model would completely be ignored.

1.3 Methodology

This thesis work has two main purposes: to give a literature review of maritime cyber and physical security, autonomous shipping, and incident management and reporting, and to design an incident data reporting model for autonomous shipping.

The literature review was done by researching papers, articles and news about these areas. The research was conducted mainly using the Tampere University of Technology (TUT) library's academic search engine Andor and Google Scholar. Google search engine was used in some cases to find specific Requests for Comments (RFC), news articles, and other publicly available documents. Here are the various search phrases that were used for the searches:

- Maritime industry in the Nordics
- Autonomous ship/shipping
- Autonomous vessel
- Autonomous vehicle
- Maritime security
- Maritime safety
- Maritime cyber security
- Maritime cyber security incident
- Incident management
- Incident reporting
- Incident sharing
- Incident data model/modeling

All the found documents were carefully examined and the best ones for this thesis' purposes were selected and used as references when writing the theory part of the thesis.

The incident data reporting model design was done through researching existing models and finding out whether they would be usable for this use case or not. A suitable data model was ultimately found and an extension for it was created to cater for the needs of this use case. Then the model's applicability was tested through different use scenarios. Some analysis and testing were also made to further validate the use of the data model.

Some inspiration for the structure of the thesis was drawn from various master's theses found in the TUT library.

1.4 Structure

This thesis consists of four major parts which are introduction, theory, model design, and model testing. Each part serves its own purpose, but they also fulfil each other to form a cohesive structure.

The introduction part introduces the topic and thesis to the reader. Its purpose is to get the reader interested and prepared for the information to come. The introduction part is the first chapter of the thesis.

The theory part consists of Chapters 2 and 3. Chapter 2 is mostly about the maritime industry. A short description of maritime industry in the Nordic countries is given. In Chapter 2.1 autonomous shipping is explained and a model ship and its equipment are introduced. Some different concepts of autonomy are introduced and compared. Possible problems that autonomous shipping and ships will face are explained. In Chapter 2.2, the current state of maritime cyber security is described. Common maritime physical and cyber security practices are introduced and reflected on autonomous shipping. Some example maritime cyber security incidents from around the world are introduced.

In the third chapter, incident management and reporting are shortly explained, and the common practices of incident reporting are introduced in Chapter 3.1. Data modeling is then explained in Chapter 3.2 and some current incident data models are previewed in Chapter 3.3. The purpose of the theory part is to give the reader interesting and useful information about the topics of the thesis and to prepare the reader for the later chapters.

The fourth chapter, which is the model design part, explains why the Incident Object Description Exchange Format (IODEF) data model was chosen for this use case. A thorough look into the specification document of the IODEF data model is given in Chapter 4.1. After the specification is examined, it is noticed that an extension is needed for the data model to be usable for our use case. This extension is then designed and explained in Chapter 4.2.

The fifth and sixth chapters are the model testing part of the thesis. In this part, the chosen data model and the designed extension are put into use through various use scenarios to determine the applicability of this data model for our use case. Full IODEF-Documents in eXtensible Markup Language (XML) for the incident reports related to these scenarios are given in the appendices. Transport tests are conducted with these XML files and the model is further analyzed to validate the use of this data model for our use case.

The seventh chapter of this thesis is there to draw conclusions about the thesis work. All the research questions are given answers here. The goal of this chapter is to draw the thesis together and make it whole.

2. THE MARITIME INDUSTRY

The Nordic countries - Finland, Sweden, Norway, Denmark and Iceland - have a strong tradition in the maritime industry, and shipping and shipbuilding are both still big contributors to their economies. All the Nordic countries have large fleets of ships that are operated under their flags. These fleets contain many new ships, which shows that the maritime industry in the Nordic countries is still going strong. Even though a lot of the shipbuilding industry has been relocated to Asia in the recent years, many ships are still designed, and shipbuilding innovations are made in the Nordic countries. [5]

The volume of maritime transportation is increasing rapidly all around the world. Recently, Asian and South American countries have risen as the leaders of the maritime industry in terms of employment and fleet sizes. This, however, doesn't mean that the Nordic countries would have been losing by any means, this only means that the growth has been faster elsewhere. The maritime industry, including shipping, shipbuilding, cargo handling at ports, design, and research, still employs many people in the Nordic countries. [6]

In the future, the Nordic maritime industry will likely have a leading role in the innovation of advanced digital maritime solutions. As the examples presented in the introduction of world's first autonomous ship testing areas in Norway and Finland show, the industry is already taking the first steps in becoming the world leader in innovation. At the heart of these new innovations are the sharing of information, seamless connectivity between assets and teams at sea and on shore, and collaborative technological solutions. [7]

This growing focus on information and connectivity will bring new challenges for the maritime cyber security sector. Maritime cyber security is a relatively new branch of cyber security and new challenges and problems are faced every day in the field. As the Nordics, and the whole world in general, are so dependent on the maritime transport of goods and passengers, maritime cyber security is becoming a critical field of study and work. Making all the Information and Communication Technology (ICT) systems more cyber secure and resilient is a key challenge for the maritime industry. [8]

The current state of affairs regarding maritime cyber security is relatively bad. The maritime industry lacks a standardized approach to cyber security and the rates of cyberattacks against the industry are increasing. Cyberattacks targeted at key ports could potentially have disastrous consequences on a global scale. Hence a global approach to cyber security in the maritime sector is needed but will take time to implement. It would be in

the interest of everyone that the industry would come together and coalesce around a set of voluntary guidelines to improve cyber resilience. [9]

2.1 Autonomous Shipping

According to the Rolls-Royce director of digital and systems Asbjørn Skaro, autonomous cargo ships will be a common sight at the high seas by 2030. For this to become reality, many things need to happen. These include economic viability, regulation changes, and the right combination and integration of technology. [2]

The idea of autonomous shipping is not a new one. Autonomous vessels have been developed, tested and researched since the 1970's. Many small autonomous or radio-controlled vessels are in use in research, coast guard, and military applications. It is apparent that huge autonomous cargo ships will be built at some point, and it seems that the time is now. Many research, and development projects are ongoing in this field right now. [10]

The removal of the human element is seen as the biggest benefit of autonomous shipping as human errors will be less likely, crew costs are decreased, and no crew accommodations are needed onboard ships. It is said that nearly 80% of marine accidents are at least in part caused by human error. Autonomous ships will make human error less likely, but it is important to remember that the human factor will still be present in autonomous ships, in different forms. The ship is of course built by humans and the algorithms and rules of the internal decision-making logic have been designed and coded by humans who make errors. The human element is also present in the shore control centers. [10]

It is also feared that removal of the human element could be a bad thing. Humans are flexible, creative, and able to adapt to surprising situations, which should have a positive impact on the safety of the system they operate. Surprising situations are a problem as it is impossible to teach a machine to react to every possible scenario in the correct manner. Therefore keeping at least some of the human element for example via the shore control center is important for the future of autonomous shipping. [10]

2.1.1 Different Concepts of Autonomy

There are different concepts of semi-autonomous operations that the ships will probably go through before reaching full autonomy. Here are a few concepts that can become a reality.

Collecting and analyzing real time sensor data with the objective of predicting the function performance and future risk of malfunction is called monitoring the health of functions. This is a predictive system and is important for the safety of the vessel and know-

ing when a proactive maintenance is needed. These kinds of decision support systems are seen as some kind of autonomy or automation and are already in wide use in the industry. [11]

In the case of fleets of ships, the master-slave concept should be a useful one. This means that there is one normal manned ship that leads the fleet and the rest of the ships are slaves that follow the master ship. The other ships are autonomous to a decree and are fully unmanned. The operations of these ships are monitored and controlled from the master ship by a team of skilled seafarers who also have competence in autonomous technology. [11]

In the captain-on-land concept, the ship is monitored and controlled by a shore control center. In this concept, the ship still lacks autonomy and is mostly controlled from the shore. This could be a stepping stone towards autonomous operations. [11]

Coming years will show which way the evolution of autonomous ships will take. A fully autonomous ship would still need to be monitored from somewhere in case something goes wrong. Very similar to the captain-on-land concept is the Maritime Unmanned Navigation through Intelligence in Networks (MUNIN) concept, however, this concept allows more autonomy for the ship [12]. The MUNIN concept is investigated further in the next chapter.

2.1.2 The MUNIN Concept

The MUNIN -project is one of the most prevalent research projects in the field of autonomous shipping. The project focuses on four specific areas:

1. Advanced sensor module
2. Autonomous navigation system
3. Autonomous engine monitoring and control system
4. Shore control center

The interworking of these modules can be seen in Figure 2. The MUNIN -project defines a deep-sea navigational process for autonomous sailing from one port to another but does not define the autonomous operation of a vessel at the port area. The information in this chapter is referenced from the MUNIN -projects document “D8.6: Final Report: Autonomous Bridge” [12] if not otherwise specified.

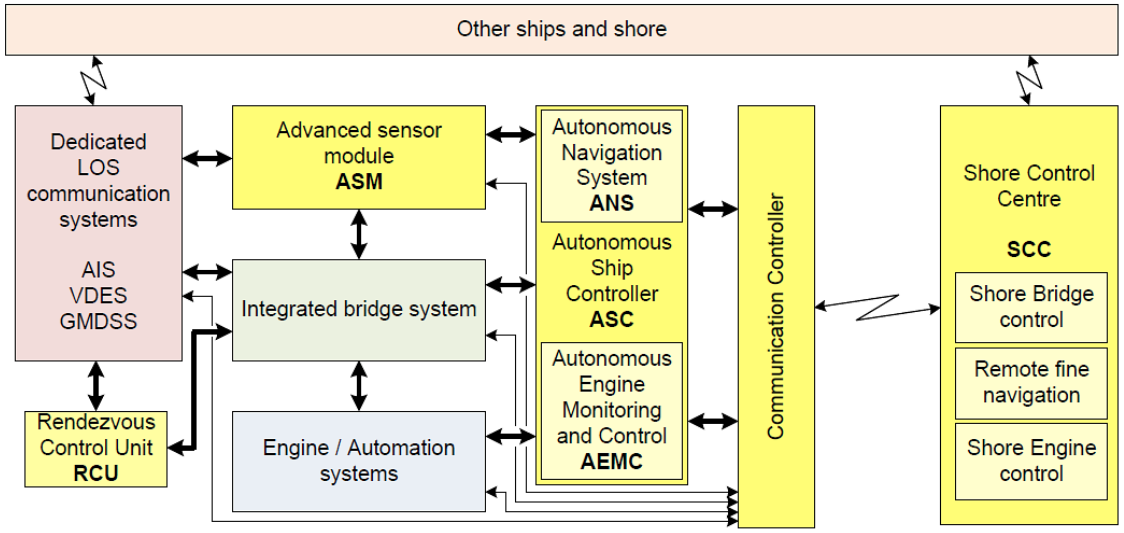

Figure 2. *Overview of the high-level MUNIN concept modules. [12]*

The advanced sensor module is used to maintain an automatic lookout for obstacles and other ships, as well as environmental conditions around the ship. The module includes and integrates the data of GPS, marine radar, Automatic Identification System (AIS) receiver, and daylight and infrared cameras. It also uses National Marine Electronics Association (NMEA) data.

NMEA 2000 is a standard for connections and data specifications between marine electronics. NMEA data includes data from all possible electronic systems of the ship. [13]

The high-level task of the autonomous navigation system is to navigate the ship from point to point safely. It works tasks such as conducting weather routing, determining ship dynamics, controlling buoyancy and stability, avoiding collisions, and managing alarms and emergencies.

The engine monitoring and control system monitors all the components of the engine room and controls the engine. It can alert the shore control center in case of critical or difficult operations that it thinks the autonomous navigation system can't handle at this moment.

The shore control center can take control of the ship if needed. In the center, operators monitor the ship and its systems around the clock. In addition to ship operators, each shore control center has a center captain who is responsible for each ship under the command of the center. There is also a center engineer who will attend technical problems. The operators report any necessary information to the captain and engineer.

This thesis will focus on autonomous ships that follow the MUNIN concept.

2.1.3 Possible Problems

There are a number of possible problems that might delay the commercial deployment of autonomous vessels. These problems range from regulatory and legal constraints to technological and financial viability, and safety concerns. The possible problems introduced in this chapter are referenced from the paper "Autonomous merchant vessels: examination of factors that impact the effective implementation of unmanned ships" [14] by Hogg et al. if not otherwise specified.

The biggest regulatory organ within the maritime industry is the International Maritime Organization (IMO). IMO has not yet been convinced that autonomous shipping is safe, so there are still no common regulations for autonomous ships. Development of regulations is expected to start in the late 2017. However, for remote-controlled and autonomous shipping to become a reality, changes at all regulatory levels are needed. Legislation at national and international levels needs to change and take autonomous shipping into account in the future. [2]

According to insurance companies, the most important thing regarding ship security is the quality of crew on board. This leads to a problem regarding insuring unmanned autonomous ships. A lot of work is needed to create new insurance policies to cover and determine duty and liability constraints for unmanned shipowners and operators.

There will be a lot of data flowing between the autonomous ship and the shore control center all the time. Most of the data will be simple sensor readings which can be sent through a cheap satellite link, but the constant data flow will still be costly. When the control center needs to take control of the ship or when high quality video feed from the ship is needed, a better satellite link is needed. These are currently rare, and the use is costly. Multiple backup connections are also needed in these critical moments. Closer to the shore cellular networks can be used which provide higher bandwidth, better quality, and lower costs. It is expected that more high quality and high bandwidth satellite links will become available in the future, but for now the connectivity at sea is a huge problem for the autonomous operation of ships.

The huge amounts of data that the shore control center receives from the ship could be a problem if not dealt with accordingly. The control center could become swamped with data and the operators would not find the data that they need to monitor the ship. The data needs to be processed and presented in a clear manner so that the operator can do his job. This requires good systems to be developed at the control centers to be able to deal with the whole dataflow and not lose any parts of the important data.

Another problem might arise from the way the industry will receive autonomous shipping. It is anticipated that there will not be instantaneous savings for shipping companies from going towards autonomy. So, the companies might not have enough incentive

to go for autonomy, which might in turn delay the era of autonomous ships. Traditional manned ships could also pose a problem for autonomous ships as no one knows how the crews will react when they encounter autonomous ships.

For autonomous shipping to become common, it needs to be economically viable. The reduced crew costs will not alone cover the needed investments, at least in the short term. The ships and the shipping chain also need to be more efficient for commercial success. This poses a great challenge for autonomous ship developers, as just developing a working autonomous ship is not enough, the ship also needs to be more efficient than the currently used cargo ships. [2]

As there is no crew onboard an autonomous ship, there is no one to perform emergency repairs if equipment fails. This means that monitoring the equipment and doing preventative maintenances will be the key to success. This also means that many critical navigation and automation systems would need to be duplicated and other redundancy be introduced in the systems of the ship. This would be costly and could be a problem for the economic viability of autonomous shipping.

Another huge problem for autonomous shipping will be physical and cyber security onboard the ships and regarding the whole maritime industry. These problems are so imperative for this thesis that they have their own subchapter right below this one.

2.2 Security Challenges at Sea

The maritime sector faces many challenges regarding cyber security. A few major problems in the field are explained below. This part of the thesis is largely a summary of chapter 2 of the European Network and Information Security Agency (ENISA) report "Analysis of Cyber Security Aspects in the Maritime Sector" [8]. The report gives a good look into the current state of cyber security in the maritime industry.

Awareness regarding cyber security is very low in the maritime sector. This applies to all the actors in the field, including government bodies, port authorities, and maritime companies. This might be caused by the yet relatively low number of cyber incidents in the sector and the low exposure these incidents receive. Yet, it is apparent that the use of ICT systems, and hence the threat of cyber incidents, is increasing in the sector and more focus on cyber security is needed. The low awareness means that a cyberattack towards any maritime ICT systems could be devastating as the incident response would likely be lacking.

The ICT systems in the maritime industry, be it at ports or on ships, are usually complex and use a large amount of different technologies. The fast development of new technology and the move towards automation and autonomy in the sector both contribute to poor cyber security in some cases. The big problem in the field is inadequate standardi-

zation and lack of good practices regarding cyber security in these ICT environments. All this leads to the fact that these systems are particularly vulnerable to cyberattacks.

A big problem within the maritime industry is that the maritime governance is highly fragmented to stakeholders on different levels. There are several global, regional, and national stakeholders in play and there is lack of coordination between these stakeholders. This brings major discrepancies in how maritime cyber security is handled and causes big differences between maritime zones. The clear definition of responsibilities and roles to be taken regarding cyber security also becomes problematic because of this fragmentation of policies and governance. Adding to this problem is ports that are being privatized, as the ICT and security standards on these ports are largely dependent on the owner of the port. If the owner doesn't care about the security aspects, they can get mostly ignored and this can cause problems in the big picture of maritime cyber security.

Maritime regulations on global, regional, and national levels currently include very little on maritime cyber security elements. These regulations mostly include safety and physical security concerns. New regulations are likely to include cyber security as well, but they are still quite far away in the future. This means that meanwhile the industry needs to work together to self-regulate the cyber security aspects. There are already some initiatives to cooperate within the industry, but this is not yet sufficient, and more work needs to be done to get the whole industry on the same page.

There is currently no holistic approach to maritime cyber security. Stakeholders are setting cyber security expectations and measures on their own and everyone is doing things differently. This leads to only a part of the risks being considered and addressed. A large portion of the risks are completely ignored, and this leaves the maritime industry vulnerable to large scale cyberattacks.

In addition to all the other problems, that maritime cyber security faces, there is also no economic incentive for the stakeholders to implement good cyber security in the maritime sector. This is caused by the fact that insurance companies have not yet taken cyber security aspects regarding the maritime sector into account. This means that there is no separate insurance for the maritime ICT systems and hence no guidelines that the implemented cyber security should follow to get the insurance payouts. This is the case in many other industries already and needs to be included in the maritime industry as well, to give the stakeholders more incentive to implement good cyber security practices.

All these challenges that maritime cyber security faces make the maritime industry a prime target for cyberattacks right now. The attackers are often motivated by monetary gain. Some attacks try to steal money directly from the affected companies while others aim at smuggling contraband cargo via penetrating the port's ICT systems. In addition, there are the attackers that aim to infiltrating, controlling, or damaging critical infra-

structure. Disrupting the shipping industry could very well have a significant economic impact on the global scale. [9]

2.2.1 Physical Security

The Maritime Security Section of IMO is responsible for giving guidelines and policies regarding physical security to the entire industry. IMO has been providing these guidelines and policies since the 1980s and continues to keep them up-to-date. This is in stark contrast to the situation with cyber security where no common regulations or guidelines are present. This chapter is a summary of IMO guidelines given in the paper "IMO Maritime Security Measures - Background" [15].

IMO's policies give governments the chance to set a security level that applies to ships and port facilities in their governance. There are 3 different security levels for different situations. Security Level 1 means normal operations. Security Level 2 means that there is a heightened risk of a security incident. Security Level 3 means that the risk of a security incident is probable or imminent.

Maritime physical security includes securing supply chains, port facilities, and ships as well as protecting the environment. All these actions are seen as risk management activities which means that risk assessment is needed in all of the cases. IMO provides the industry with standardized and consistent framework for evaluating and responding to risks. In addition to the risk assessment and management, there are also some minimum functional security requirements for ports and ships. For ships, these requirements include:

1. Ship security plans
2. Ship security officers
3. Company security officers
4. Certain onboard equipment
5. Monitoring and controlling access
6. Monitoring the activities of people and cargo
7. Ensuring that security communications are readily available

There are also similar requirements for port facilities, but this thesis will focus on the case of ships as per the scope set in Chapter 1. These requirements are further explained in the coming paragraphs.

The ship security plan specifies the minimum operational and physical security measures that the ship needs to take always. This includes operations at Security Level 1. The plan also indicates the additional security measures that need to be taken to get the ship to Security Level 2. For Security Level 3 the plan specifies the preparatory actions that need to be taken so that the ship can swiftly respond to a security incident or

threat. The ship security plan and any changes to it need to be approved by the administrator of the ship.

Every shipping company needs to appoint a company security officer and a ship security officer for each of their ships. The security officers have many responsibilities including ensuring that the ship security assessment is undertaken, and the ship security plan is prepared. They also monitor the effectiveness of the ship security plan and ensure that the plan is followed. All their responsibilities are defined in IMO's guidelines.

Examples of required onboard equipment include automatic identification systems and ship security alert systems. The automatic identification system provides information like the unique identification, position, course, and speed of the ship. The ship security alert system is used by seafarers to notify other ships and autorities of a terrorist hijacking.

Monitoring and controlling physical access to the ship at port and at sea depend largely on risk assessment. Different equipment for this purpose is used for example in different regions and with different ship types. Seafarer identification documents are also an important part of access control. Monitoring the activities of people and cargo is the responsibility of the ship security officer. Most ships are fitted with security cameras for monitoring purposes, but this is not required.

All of these requirements seem important also in the case of autonomous ships. Especially the requirement for readily available security communications is interesting for this thesis. Of course, the requirements need to be specified for the case of autonomous ships later. For example, even though there is no one on board the ship, there can be a ship security officer at the control center.

In the case of autonomous ships, the physical security threats are little different than in traditional shipping. There is no crew, so the protection of crew is not required. The vulnerable parts in an autonomous ship would be the cargo and the ship itself. The biggest physical threats at sea would probably be the stealing of cargo and attacks meant to damage the ship in some way. Another threat would be traditional ships and vessels as it is impossible to know how the crews react to autonomous ships. At ports, the biggest threat is unauthorized access to the ship and possible tampering with its equipment.

2.2.2 Cyber Security

By now it is apparent that cyber security is still a problematic thing in the maritime industry. Clear policies and regulations on cyber security onboard ships and at ports are missing. IMO has only just recently started giving high-level recommendations on maritime cyber risk management, the latest draft being from July 2017 [16]. These are basic recommendations and a lot of work is needed before IMO can provide the industry with

real policies. There are, however, some guidelines on cyber security developed by companies and organizations in the industry based on IMO's recommendations.

Here we take a look at these guidelines to see the threats and vulnerabilities that there are considering cyber security onboard ships. We also consider possible preventative measures and fixes for these threats and vulnerabilities. This chapter is mostly referenced from the paper "The Guidelines on Cyber Security Onboard Ships" [17], which has been written in collaboration by many of the biggest companies in the maritime industry.

Cyber security should always be a part of the risk assessment and management in both company and ship levels. According to "The Guidelines on Cyber Security Onboard Ships", cyber risk management should:

- identify the roles and responsibilities of users, key personnel, and management both ashore and on board.
- identify the systems, assets, data, and capabilities, which if disrupted, could pose risks to the operations and safety of the ship.
- implement technical measures to protect against a cyber incident and ensure the continuity of operations. This may include the configuration of networks, access control to networks and systems, communication and boundary defense, and the use of protection and detection software.
- implement activities and plans (procedural protection measures) to provide resilience against cyber incidents. This may include training and increasing awareness, software maintenance, remote and local access, access privileges, use of removable media, and equipment disposal.
- implement activities to prepare for and respond to cyber incidents.

This is very similar to physical security management but requires technical knowledge of cyber security and ICT systems.

It is recommended to use multiple layers of protective measures to make the systems cyber resilient. Using multiple layers of protection increases the probability that a cyber incident is detected and removes a considerable number of false positives. A combination of physical security of the ship, protection of networks, intrusion detection, software whitelisting, access and user controls, password policies, and personnel awareness of risks will result in good cyber resilience. Onboard ships, where integration between cyber systems is high, it is also important to prevent vulnerabilities in a system that can be used to gain access to another system.

Different groups or individuals are interested in exploiting any cyber vulnerabilities a ship might have, for different reasons. Even a company's own employee might unintentionally compromise cyber systems or data while working on the company's ICT sys-

tems. Table 1 contains different groups, their motivation for exploiting cyber vulnerabilities, and the goals they want to reach by exploiting them.

Table 1. *Groups exploiting cyber vulnerabilities. [17]*

Group	**Motivation**	**Objective**
Activists	Reputational damage, Disruption of operations	Destruction of data, Publication of sensitive data, Media attention, Denial of access to service or system
Criminals	Financial gain, Commercial espionage, Industrial espionage	Selling stolen data, Ransoming stolen data or systems, Arranging transportation of contraband cargo, Gathering intelligence for another crime
Opportunists	The challenge	Getting through cyber security defenses, Financial gain
State sponsored organizations, Terrorists	Political gain, Espionage	Gaining knowledge, Disruption to economies and critical national infrastructure
Company employees	Dissatisfaction with the company, Human error	Damaging the company or the ship

There are two types of possible cyberattacks that can affect ships. These are targeted and untargeted attacks. In a targeted attack the ship is the intended target, whereas in an untargeted attack the ship is one of many possible targets. Untargeted attacks usually exploit known vulnerabilities that might exist in some systems that the ship uses. Tools for untargeted attacks are widely available in the Internet. Here are some examples of these tools:

- Malware
- Social engineering
- Phishing
- Watering hole attack
- Scanning

Targeted attacks, however, often use tools and techniques specifically tailored to attack this exact ship. Here are some examples of these tools:

- Brute force
- Denial of service

- Spear-phishing
- Subverting the supply chain

These examples are of course not exhaustive and only show the most commonly used tools and techniques. The tools and techniques are always evolving to counteract the evolving of cyber security. New kinds of attacks are observed every year.

Most cyberattacks are conducted on stages. First stage is surveying or reconnaissance, where information is collected about the target ship or company. Second stage is delivery, where the attacker attempts to access the systems of the ship. The third stage is breach, where the attacker gains access to some of the equipment of the ship. The last stage is effect, where the attacker does what he came to do to the breached system. Most cyberattacks are stopped during the second or third stages thanks to good cyber security on the targeted system.

Ships and especially autonomous ships have a large amount of systems onboard. Any of these systems could potentially be vulnerable to a cyberattack. Here is a list of potentially vulnerable systems onboard ships:

- Communication systems
- Bridge systems
- Propulsion and machinery management and power control systems
- Access control systems
- Cargo management systems
- Core infrastructure systems

There is a list of equipment that these systems might include in Appendix A.

Recently, ships have grown more reliant on the ship-to-shore interface, which is nowadays used to conduct many different tasks. Especially with the introduction of autonomous ships this interface and the satellite link will see even more use and be a key system to protect from cyberattacks.

2.2.3 Cyber Threats Specific to Autonomous Shipping

Autonomous ships are such a new thing that not much research has yet been done about cyber threats specifically concerning them. There is, however, some research about cyber threats towards autonomous vehicles. Here we take a look at the paper “Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges” [18] by Parkinson et al. that focuses on threats towards autonomous cars. These threats are examined hypothetically in the autonomous shipping world.

In the case of autonomous vehicles, it was discovered that many vulnerabilities lie in the different sensor systems that the vehicle uses to get information about its surroundings, position, speed, etc. In the case of the MUNIN concept of autonomous vessels it would mean that the advanced sensor module is vulnerable to cyber threats. This is probably true as the advanced sensor module contains many similar or same sensors that an autonomous vehicle does, and hence will have similar vulnerabilities. All the sensors in the advanced sensor module are susceptible to getting false data fed to them. This kind of attack usually requires the attacker to have physical access to the sensor, but it is also possible to hack into the connections and to falsify the data feed. False sensor data could have all kinds of effects in the other systems of the vessel.

GPS spoofing where a strong counterfeit GPS signal is generated and directed towards the vessel could be a possible attack scenario. This counterfeit signal would overtake the real GPS signals as GPS is usually set to use the strongest signal. This could cause the vessel to take course wherever the attackers want the vessel to go. Another attack scenario could be GPS jamming where radio noise is broadcast on the GPS frequency. This noise blocks the use of GPS and could disable the vessel's ability to navigate.

Light Detection and Ranging (LIDAR) sensors are used to measure distance to objects and to produce a 3D map of the environment. This is used for localization, obstacle avoidance, and navigation. LIDAR measures the flight time of a pulse of light to measure the distance between a sensor and an object. LIDAR spoofing or jamming is easy to do with low cost equipment, namely pointing a laser at the right frequency towards the LIDAR receiver. This can cause the vessel to think that there is a big object ahead and that it needs to stop. This attack requires the attacker to be close and can be used to board the autonomous vessel.

Daylight and infrared cameras are used for a similar purpose as LIDAR. These cameras can be disabled by simply shining a bright light at them. A bright enough light could also accidentally get reflected towards the cameras to temporarily disable them. This could easily cause the vessel not to detect an obstacle ahead and a crash could happen.

The autonomous engine monitoring and control system and the autonomous navigation system of the MUNIN concept have similar functions and uses as the several engine control units in an autonomous vehicle. The engine control units of an autonomous vehicle have several tens of millions of lines of code between them, so a huge amount of lines of code could be assumed for the systems of an autonomous vessel as well. Such a huge amount of code makes code reviews infeasible and many vulnerabilities in the code are there just waiting to be found. Many such vulnerabilities have been found in the case of autonomous vehicles and it is evident that vulnerabilities will also exist in the case of autonomous vessels.

In the MUNIN concept, the shore control center could also be susceptible to cyberattacks. An attacker could gain access to the systems of the control center and could affect the ship that way. Also, intercepting the communications between the ship and the control center and possibly changing the communications could be a possibility. It is important to notice that cyber security implications affect the whole system of a ship connected to the control center, instead of only affecting the ship.

2.2.4 Example Incidents

Maritime cyberattacks are becoming quite common because maritime cyber security is lacking, and the maritime industry is hence seen as an easy target. Many of these incidents are, however, not reported at all and just kept inside the company. Here are some incidents that have been reported from around the world.

Belgium, 2011

There was a big cyberattack towards the port of Antwerp going on between 2011 and 2013. Drug smugglers had employed hackers to hack into the port's systems to allow them access to secure data about locations and security details of containers. This allowed the drug traffickers to place heroin and cocaine inside seemingly legitimate containers that they could then empty before anyone would suspect anything. This plot was going strong for about two years, but eventually the security breach was discovered and at least some of the criminals involved were brought to justice. Similar attacks are most likely ongoing right now elsewhere in the world and some have been discovered since the Antwerp incident. These kinds of attack have been coined "ghost shipping". [19]

Global, 2017

In 2017 a computer virus affected the ICT systems of the world's biggest container shipping line and operator of tens of ports, Maersk. The attack caused many of Maersk's ICT systems to shut down completely and crippled its operations for several days. Cargo ports all around the world were closed as normal operations could not be carried out. The ports had lost all information about what cargo each container contained, so it was impossible to deliver or receive any cargo until the ICT systems were operational once again. It took Maersk days until operations were back to normal at their ports and this caused big problems in the logistic chains of many cargo owners across the world. [20]

India, 2012

In 2012, two separate incidents happened off the coast of India. In the first incident, two Indian fishermen were shot by Italian marines on board a merchant vessel because the fishermen were thought to be pirates attacking the merchant vessel. In the second incident, three fishermen were killed in a hit-and-run accident. What makes these incidents

similar and related to cyber security, however, is the fact that in both cases the data collected by the Voyage Data Recorder (VDR) was corrupted or lost. A VDR is a device that records crucial data about the position and speed of the ship, as well as audio recordings from the bridge, and radar images. It can be likened to a black box on airplanes. In both cases it is suspected that the crews of the ships had tampered with the VDRs to conceal their wrongdoings. This can be seen as a cyberattack towards the equipment of the ship. [21]

Singapore, 2017

A collision between the US navy destroyer USS McCain and a merchant vessel called Alnic MC took place off the coast of Singapore in 2017. As a result of the collision, 10 sailors aboard the USS McCain were killed and 5 were injured. At first there were speculations that a cyberattack targeted at the USS McCain caused the collision, but these claims were quickly dismissed by the US navy. A new hypothesis has surfaced since, that claims that the merchant vessel Alnic MC was the target of a cyberattack that caused the collision. This has not yet been confirmed or denied but it seems more likely, since commercial equipment is way easier to hack into than military equipment. This was the fourth incident this year involving a US navy ship and the second similar incident in quick succession. This has sparked speculations that the US navy is a target of some kind of an attack and the navy has tightened its cyber security and added cyber causes to the list of things they investigate relating to any incident. [22]

Russia, 2017

At least 20 ships were affected by a GPS spoofing attack in the Black Sea in 2017. According to GPS all the ships were over 32 kilometers inland at Gelendzhik Airport. The false GPS signal thankfully didn’t cause any collisions or damages to the affected ships. Experts think that this was the first case of GPS spoofing ever documented outside of controlled tests. It has been speculated that the spoofing attack was caused by Russia testing new electronic warfare technologies. [23]

3. INCIDENT MANAGEMENT AND REPORTING

A cyber security incident is an event that disrupts normal operations. It may indicate that an organization's network, ICT systems, or data have been compromised or that a protective measure set in place to protect these has failed. The International Organization for Standardization (ISO) standard for information security incident management, ISO/IEC 27035-1:2016, defines an information security incident as follows: *"One or multiple related and identified information security events that can harm an organization's assets or compromise its operations."* [24] and the National Institute of Standards and Technology (NIST) computer security incident handling guide, NIST Special Publication 800-61, defines it as: *"A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices."* [25].

A cyber security incident can result in multiple negative impacts, for example financial loss, legal issues, loss of productivity, or loss of company reputation [26]. These incidents need to be managed to minimize the negative impact on the organization. Information security incident management is quite heavily standardized and the two standard approaches that stand out the most are the ISO/IEC 27035-1:2016 [24] and the NIST Special Publication 800-61 [25]. They both offer a similar structure for incident management.

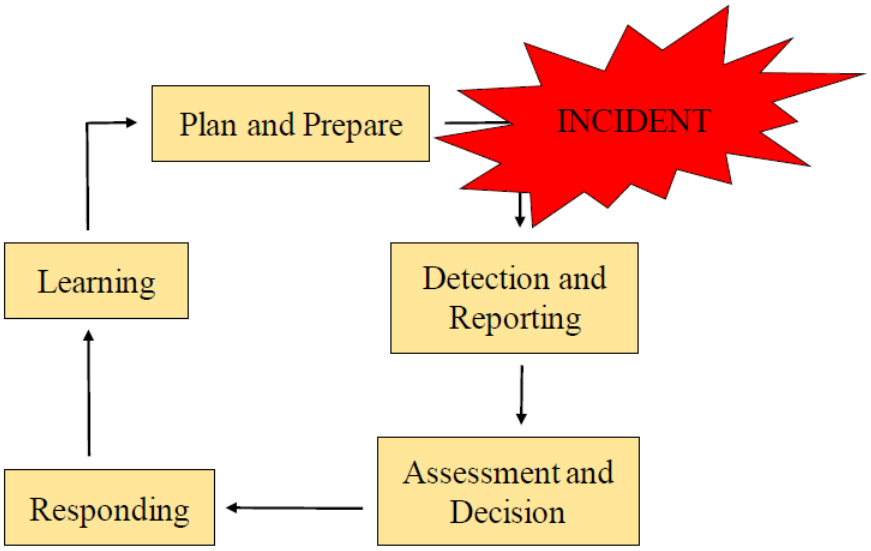

Figure 3. *Incident management life cycle.*

As seen in Figure 3, incident management can be both proactive and reactive. The proactive part includes planning, preparing and risk assessment. It is there to prevent incidents, to raise awareness within the organization, and to make sure that the organization

is ready to act when an incident takes place. The reactive part kicks in when an incident occurs and lasts until normal operations are restored. It includes detecting the incident, collecting data about it, reporting the incident to the right audience, assessing and validating it, containing the incident, choosing the right actions and acting on them, recovering from the incident, and learning from it. After that it is right back to the proactive part and setting up preventative measures so that a similar incident won't happen again. [26]

3.1 The Common Practices of Incident Reporting

For this thesis' purposes the most interesting parts of the incident reporting and management process are the detection and reporting phase, and the assessment and validation phase. A linear model of the incident reporting and handling process can be seen in Figure 4. The parts that we are interested in are shown in green and the rest are greyed out.

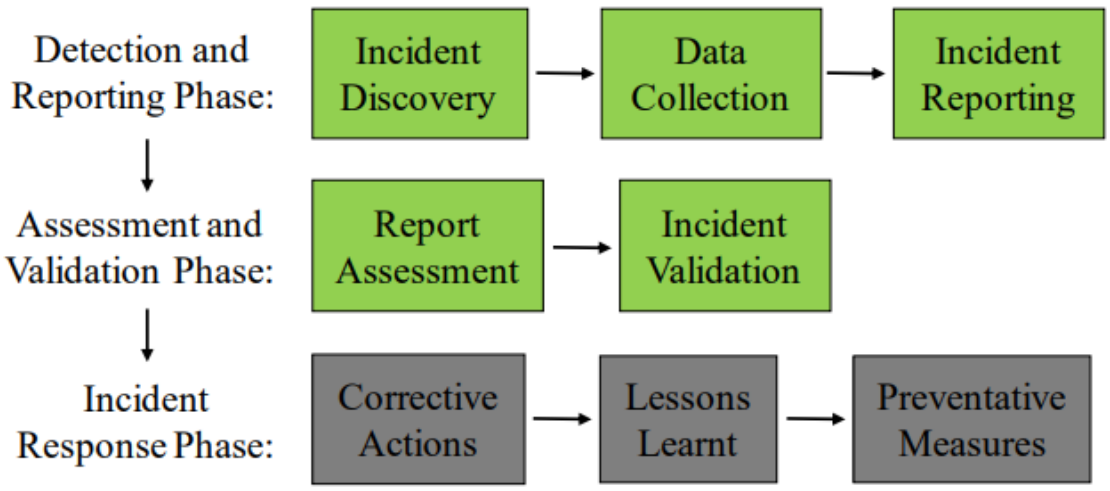

Figure 4. *The phases of the incident reporting and handling process.*

Incident detection, reporting, and validation can all happen either manually or automatically. Here is a list of some sources where incidents can be detected:

- Alerts from security monitoring systems such as intrusion detection (and prevention) systems, antivirus software, honeypots, log monitoring systems, security information and event management systems, and correlation engines.
- Alerts from network monitoring systems such as firewalls, network flow analysis, and web filtering.
- Analysis of log information from various systems and devices.
- User reports and notifications from third parties.

This list is gotten from the article "Information Security Incident Management: Current Practice as Reported in the Literature" [26] by Tøndel et al.

After an incident is detected, all possible data about it should be collected from all possible sources and stored securely. Then all the relevant information about the incident should be made available in some kind of an incident tracking solution, with date and time of the incident. [26]

In all cases it is not so straightforward to know where an incident needs to be reported [27]. In our case of incidents happening on an autonomous ship, however, it is straightforward that the incident needs to be reported to the shore control center responsible for the ship. These incidents are mostly discovered and reported by either the equipment of the ship or by the equipment or personnel of the control center, rather than an outside observer. If the incident can't be solved in-house or it affects people outside the organization, the incident is further reported, perhaps to the national Computer Security Incident Response Team (CSIRT) or any other valid audience [27].

In the assessment and validation phase, all the information about the incident is assessed and a decision is made whether the event is an information security incident or a false positive [26]. Three different incident discovery and validation schemes are shown in Figure 5. In the figure, the red number ones indicate the entry point for the incident response process.

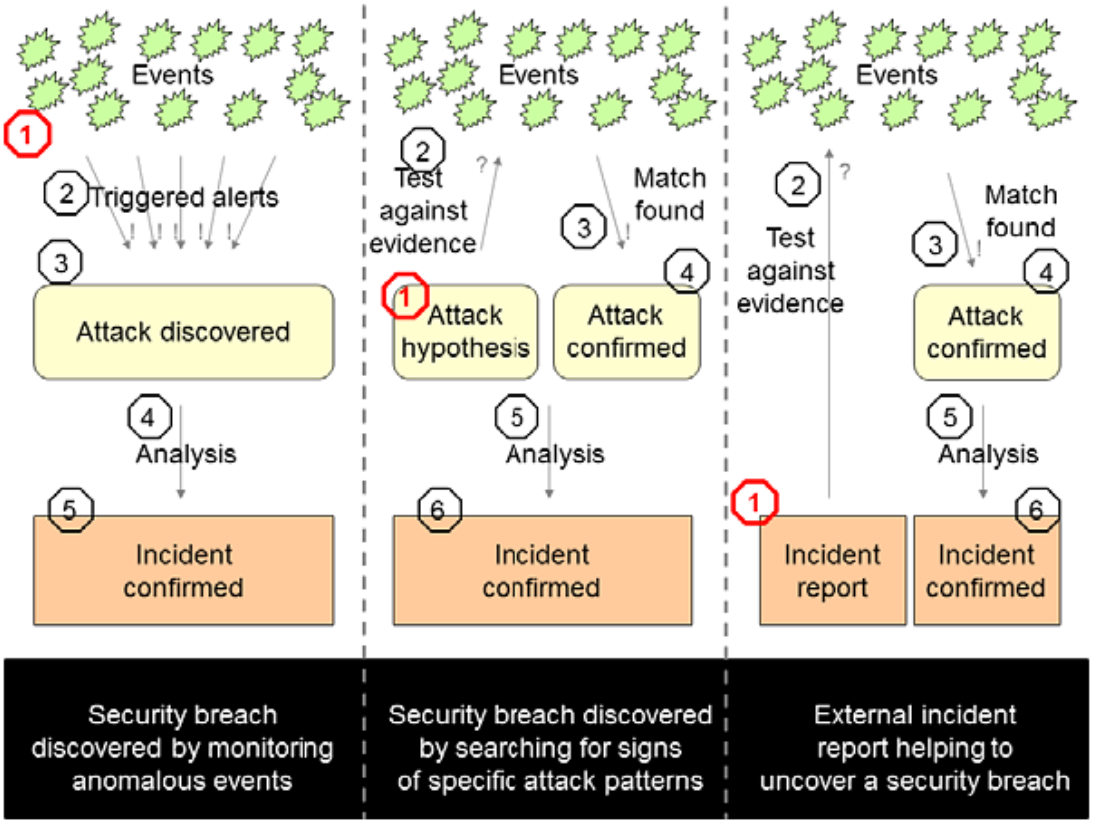

Figure 5. *Schemes of incident discovery and validation. [27]*

After a real incident is detected, the organization's CSIRT decides how the incident should be addressed, who should do it, and with what priority. The organization should

have a classification scale for incidents, based on impact on affected systems and assets, to help prioritize incident management. After these decisions are made, the right personnel are contacted and given their assignments and the incident response phase can start. [26]

3.2 Data Modeling

Data modeling is the act of representing real-world facts as symbols or codes and organizing them into tables and columns in a database [28]. For example, time can be represented in countless formats, but the model ensures that the format is the same every time in this particular database.

A well-designed data model can give the organization leverage in a sense that it can make the programming and designing of the rest of the organization's ICT systems cheaper and easier. Also, a poor data model can become costly as changes to data models will incur huge costs as other systems need to be changed as well. Data modeling helps represent data in a more concise format. This means that only important data is present and easily accessible. Data modeling also improves data quality as inaccurate data is easier to spot and remove. [28]

There are certain characteristics that a good data model fulfils. Here are some of them:

- Completeness, in a sense that the model supports all the data that is necessary for the system.
- Non-redundancy, meaning no data is represented in two or more separate locations.
- Enforcement of business rules, for example two incidents can't have the same incident ID.
- Data reusability, in a sense that the data should be usable in other applications than the originally intended one as well.
- Stability and flexibility, meaning the model's ability to adapt to changing business requirements.
- Elegance, as in neat and simple classification of the data.
- Communication, meaning that the data is easily shareable with various stakeholders.

Fulfilling all the above characteristics would be great but probably not realistic. A good balance between the characteristics makes a good data model. Performance could also be seen as one of the important characteristics of a good data model, but it is so heavily dependent on the software and hardware platforms on which the database will run that it really differs from the aforementioned characteristics. [28]

3.3 Current Methods of Incident Data Modeling and Sharing

Even today, many security incidents are handled by humans using human-readable data models that are specific to organizations [27]. However, automation is a growing trend and many machine-readable data models are being developed. This means that machine-readable data models are used, and the data is formatted into human-readable form when needed.

Data modeling is needed so that the incident data can be represented in a concise and precise manner. Using a data model also ensures that all the important data about an incident is collected. Sometimes companies also share incident data with each other [27]. This is done so that similar incidents can be prevented from happening or can be reacted to faster elsewhere. It could be argued that a data model that is machine-readable, widely used, and easy to convert to a form that is readable by humans would be the best.

In the following chapters a couple of these machine-readable incident data modeling and sharing methods are described. The focus is kept on the data models, but the data sharing methods that are developed with the data models are also shortly explained.

3.3.1 IODEF

Incident Object Description Exchange Format (IODEF) is an information framework to represent computer and network security incidents. It is being developed by the Managed Incident Lightweight Exchange (MILE) working group of the Internet Engineering Task Force (IETF). MILE also develops Real-time Inter-network Defense (RID) and Resource-Oriented Lightweight Information Exchange (ROLIE) which both are tools of incident data sharing. [29]

The MILE working group develops standards to support computer and network security incident management. They focus on data models and transport protocols to enable the secure exchange of incident information. Although the data models and transport protocols are developed together they can be used independently. This means that the data model could be used with different transport methods and the transport protocols could be used to transport information formatted in different data models. [30]

Version 2 of IODEF is defined in RFC 7970 as *"A data representation for security incident reports and indicators commonly exchanged by operational security teams for mitigation and watch and warning."* [31]. The RFC provides IODEF's data model specified with the XML schema. Recently, the MILE working group has also started working on providing the data model in JavaScript Object Notation (JSON) format [32].

The highest-level object of the IODEF data model is the IODEF-Document class. It contains attributes for version, language, schema, and so on. The aggregate classes of this class are Incident and AdditionalData. There can be one or more of the Incident class and each of them contains information related to a single incident. The AdditionalData class can be used to apply extensions, there can be zero or more of these. [31]

The Incident class contains multiple attributes and has a wide variety of aggregate classes [31]. Information like incident ID, detection time, reporting time, description and event data can be found inside the incident class. The descriptions of all the attributes and aggregate classes can be found in RFC 7970. A representation of the Incident class can be found in Figure 6.

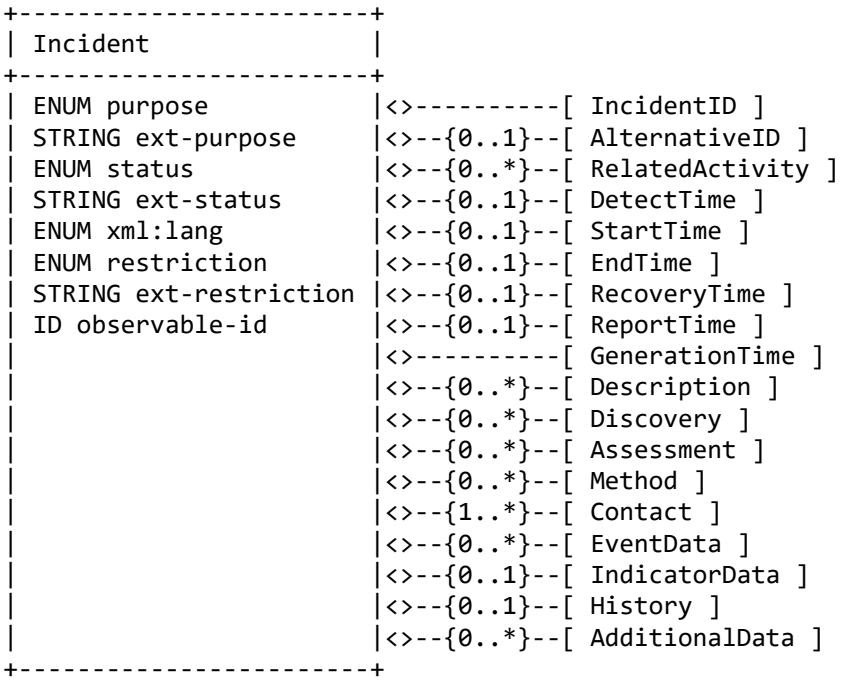

Figure 6. *A representation of the IODEF Incident class. [31]*

Guidelines to defining extensions to IODEF are explained in RFC 6684. The extensions can be used to include industry-specific data in the data model of IODEF. Before defining an extension, it is important to go through the IODEF specifications and ensure that this data can't already be included in the data model somehow, as IODEF has a wide set of incident-related classes. Some extensions can be made public by MILE and some stay organization specific. [33]

RFC 6545 defines RID and it is described as *"A proactive inter-network communication method to facilitate sharing incident-handling data while integrating existing detection, tracing, source identification, and mitigation mechanisms for a complete incident-handling solution."* [34]. RID can be used to transport incident data between known

peers when high levels of security and privacy are needed [30]. RID is mainly used as a point-to-point transport protocol.

ROLIE can be used for the publication, sharing, or discovery of security automation information. The point is to provide access to a repository of security automation information in IODEF or other data format. The access can be restricted to internal use or it can be completely public. All the information is organized, categorized, and described, and the user can search through the information that he has access to. [35]

3.3.2 STIX

Structured Threat Information Expression (STIX) is a language and serialization format used to exchange cyber threat intelligence. It is being developed by the OASIS cyber threat intelligence technical committee. OASIS is a non-profit consortium that tries to advance open standards for the information society. The technical committee also develops Trusted Automated Exchange of Intelligence Information (TAXII) that is a protocol used to exchange cyber threat intelligence. [36]

The STIX data model is represented in JSON format. The model is machine-readable and easily convertible to a human-readable form. The data model consists of objects that can contain all kinds of information about the described cyber threat. The two types of objects are domain objects and relationship objects. These form a connected graph of nodes and edges, domain objects being the nodes and relationship objects the edges. A list of STIX objects and their short descriptions are provided in Table 2. [37]

Table 2. *STIX objects and their descriptions. [38]*

Domain Objects	**Description**
Attack Pattern	Ways threat actors try to compromise targets.
Campaign	A set of malicious activities or attacks that occur over a period of time against a specific set of targets.
Course of Action	An action taken to either prevent an attack or respond to an attack.
Identity	Individuals, organizations or groups.
Indicator	A pattern that can be used to detect suspicious or malicious cyber activity.
Intrusion Set	A grouped set of adversarial behaviors and resources with common properties believed to be orchestrated by a single threat actor.
Malware	Malicious code and malicious software, used to compromise the confidentiality, integrity, or availability of a victim's data or system.
Observed Data	Conveys information observed on a system or network.

Report	Collections of threat intelligence focused on one or more topics, such as a description of a threat actor, malware, or attack technique, including contextual details.
Threat Actor	Individuals, groups, or organizations believed to be operating with malicious intent.
Tool	Legitimate software that can be used by threat actors to perform attacks.
Vulnerability	A mistake in software that can be directly used by a hacker to gain access to a system or network.
Relationship Objects	**Description**
Relationship	Used to link two Domain Objects and to describe how they are related to each other.
Sighting	Denotes the belief that an element of cyber threat intelligence was seen (e.g., indicator, malware).

All the STIX objects contain properties that describe the object. These can include type, name, id, time created, and many more. In addition to properties, the domain objects can contain relationships with each other. These are described with relationship objects that are embedded in the domain objects. [39]

STIX has many specific vocabularies to be used with objects. All the data types, full object descriptions, and vocabularies can be found in the STIX specifications. STIX can also be customized for specific use cases with custom properties and custom objects. The STIX data model schema is provided in JSON format. [37]

TAXII is an application layer protocol for the communication of cyber threat information in a simple and scalable manner. It is mainly meant for sharing cyber threat information between organizations. TAXII defines two primary services:

- **Collection:** A repository of cyber threat information that can be accessed by clients via a request-response model.
- **Channel:** A server to which cyber threat information can be published and the information is distributed to subscribing clients.

TAXII is developed with STIX, but they are not required to be used together and can see individual use with different data models or transport methods. [40]

3.3.3 VERIS

The Vocabulary for Event Recording and Incident Sharing (VERIS) is a set of metrics designed to provide a common language for describing security incidents in a structured and repeatable manner, developed by the VERIS community. The goal of VERIS is to

collect incident-specific data and to share that with others in an anonymous and responsible manner. The VERIS community provides an open and free repository of incident information in VERIS format. [41]

The VERIS data model is represented in JSON, which makes it machine-readable. However, lots of work has gone into making the VERIS schema easily readable by humans as well. The VERIS schema is organized into five major sections:

- Incident tracking
- Victim demographics
- Incident description
- Discovery & response
- Impact assessment

Each section contains multiple items that describe the incident. The full list of items on each section can be found in the VERIS schema documentation. [41]

The VERIS schema provides enough information about an incident that it can be used for preventing further attacks, but it doesn't provide things like indicators of compromise and other technical data. The focus is on strategic and risk-based information and as such the VERIS schema should only be used as a tool to share information with other organizations, rather than using it as an incident reporting tool within the organization. [41]

4. INCIDENT DATA REPORTING MODEL DESIGN

As explained in Chapter 2, autonomous shipping is a new and developing industry, and many things in the field don't yet have common practices. This includes incident data reporting. Based on this, it is important to research and test different data models to find the most suitable one for this use case. There are also some specialties that come with this use case, especially the fact that the target of cyberattacks is moving. This leads to us probably wanting some positional information, like GPS data, in the incident data model.

During the research phase for Chapters 2 and 3, it became apparent that good incident data reporting models already exist. This means that designing a completely new model would be redundant and a waste of time. Instead, an existing model is applied for our use case. This is done by thoroughly examining the existing model and ensuring that it can represent all the data that is needed for the use case of reporting an incident from an autonomous ship to the shore control center.

Especially IODEF seems like a great fit for this use case. The IODEF data model has a vast number of classes to describe incidents and it can even be complemented with extensions to provide case specific classes and attributes. IODEF is also specifically designed to be a format for transporting data [31], and not storing it, and that is exactly what is needed here. It is available in both XML and JSON formats, so organizations can choose their preferred format. IODEF is also the closest thing to a standard in the field right now as it is developed by an IETF working group, and the RFC for IODEF is already labeled as a proposed standard.

This chapter provides insight into what the data model should be able to represent. The IODEF specification is also looked into more closely. It is also investigated whether an extension is needed for this use case or not. If an extension is needed, a basic design for an extension is given in this chapter as well.

4.1 Examining the IODEF Specification

In this chapter the IODEF specification document RFC 7970 [31] is thoroughly examined to see what kind of attributes can be represented with the IODEF data model. The goal is to determine whether all the needed attributes for our use case are already present in the model or not. If not, it means we need to design an extension to include any attributes that are needed but are currently missing from the model.

In IODEF, the Incident class is used to represent information relating to a single incident. The IODEF-Document class can be used to tie these incidents together. Here the focus is on the Incident class and what can be represented within it.

The Incident class itself has some useful attributes, like the purpose attribute, which is used to represent the purpose of the incident data report. The possible values of this are traceback, mitigation, reporting, watch, and other. Basically, this attribute is used to evaluate what needs to be done regarding the incident. Another useful attribute is the status attribute. It can have values like new, in-progress, forwarded, resolved, and future. The class also has a language identifier attribute and an attribute to indicate disclosure guidelines for the class.

The disclosure guidelines are represented in the restriction attribute, which is a common attribute within the IODEF data model. Each class of the model, even the aggregate classes, have a restriction attribute. The default value of this attribute is private, but it can have values like public, partner, and need-to-know. This is a useful attribute to see who the information should be shared with.

In addition to attributes, the Incident class also has a wide variety of aggregate classes that can be used to represent all kinds of things. Most of the classes are optional, some are required, and some can even have multiple instances. In the following, the aggregate classes are examined.

IncidentID Class

This class is used as an identifier for the incident within the CSIRT, in this case the control center of the autonomous ship. The incident ID is represented as a string value and it must be unique within the CSIRT. The class also has an attribute called name, which identifies the CSIRT generating the incident report. This class is something that should be in every incident data model, as having an identifier for each incident is extremely important. In the IODEF data model, this class is required.

AlternativeID Class

This class is used to track IDs that other CSIRTs use for the same incident. This class has one or more of the IncidentID class as aggregate classes. This class is optional. Using this class should be considered when working together with another or multiple CSIRTs to solve an incident.

RelatedActivity Class

This class is used to relate the incident to previously observed incidents or activity. It also allows to attribute the incident to a specific actor or campaign. This class is optional, but should be useful for grouping similar incidents together, when information about

previous incidents can be useful for incident management purposes, or when the same actor is continuously attacking the same target or area.

The Time Classes

The Incident class contains several aggregate classes containing information about a specific time instant. These are all represented in the Date-Time String format that is specified in the RFC. The time classes are:

- **DetectTime:** The time the incident was first detected.
- **StartTime:** The time the incident started.
- **EndTime:** The time the incident ended.
- **RecoveryTime:** The time the site recovered from the incident.
- **ReportTime:** The time the incident was reported.
- **GenerationTime:** The time the contents in this Incident class were generated.

Out of these, only the GenerationTime class is required by the data model, the rest are optional. While these time classes are certainly useful and interesting information, they are not indeed required for successful incident management. The GenerationTime class is probably the most important from the incident reporting standpoint as well, DetectTime following as a close second.

Description Class

This class contains a free form description of the incident. This is optional, but certainly useful in some cases, especially when the incident report is generated by a human. Automatically generated incident reports could have something like keywords instead of a free form description, to describe the incident. These keywords could include, among others, “connection disrupted”, “data compromised”, “systems unavailable”, and so on.

Discovery Class

This class describes how an incident was detected. This class has an attribute called source that has 20 different possible values that can describe the source of the incident detection. These include, among others, intrusion detection systems, third-party monitoring, log data, and manual investigation. In addition to this, a free form description of how the incident was detected can be given. This class can also have a Contact class as aggregate class to specify the contact information of the person or organization that discovered the incident. Another aggregate class is DetectionPattern which describes an application-specific configuration that was used to detect the incident in either free form or machine-readable form. The information in this class is really important and useful for incident management purposes. Of course, this information isn’t always known and hence the class is marked as optional.

Assessment Class

This class describes the repercussions of the incident to the victim. Things like system impact, monetary impact, time impact, cause, and so on can be described within this class. This class can be used to describe either actual or potential outcomes, which is specified in the occurrence attribute. All the information in this class is only available after an incident is fully dealt with. Hence this class is only useful for incident sharing purposes and is marked as an optional class.

Method Class

This class describes the tactics, techniques, and procedures used, or the weaknesses exploited by the attacker in an incident. This class can contain a free form description as well as references to the used vulnerability, malware sample, advisory or an attack technique. The reference is often a Uniform Resource Locator (URL). This class is optional. The information contained in this class is often not known when generating the initial incident report. This would mean that this class is mostly useful for incident sharing purposes.

Contact Class

This class allows sharing the contact information of personnel and organizations that are involved in the incident management process. For example, names, telephone numbers, email addresses, and roles in the incident management can be specified. This is a required class within the IODEF data model. For our use case this class is not the most useful, however, as most of the incident reports are generated automatically by the equipment of the autonomous ship. Of course, this could be prefilled with the contact information of the person responsible for incident management at the shore control center, for example. For cases when incident reports are generated by operators at the control center this is useful, as well as when working with other CSIRTs.

EventData Class

This is a container class to organize data about events that happened during an incident. This contains a free form description, different time classes, and other defining information for the event. The EventData class is fairly similar to the Incident class but provides information about a single event inside the incident. There are also some special aggregate classes like Flow, Expectation, and Record. The Flow class describes the systems and networks involved in the event. The Expectation class describes the expected action to be performed by the recipient. The Record class contains additional data, for example log files, about the incident. The EventData class is recursive, i.e. the EventData class for the second event of the incident is contained as an aggregate class in the first events EventData class, third in the second and so on. This class is marked as optional but could be useful for incident reporting in some cases.

IndicatorData Class

This class describes indicators and metadata associated with them. This is how indicators are described in RFC 7970: *"An indicator consists of observable features and phenomenon that aid in the forensic or proactive detection of malicious activity and associated metadata."* [31]. The IndicatorData class can contain multiple Indicator classes. Each indicator is specified by an ID. They also include a free form description and many other useful attributes. The IndicatorData class is optional and the information contained is mostly useful for incident sharing and preventing and discovering further incidents. This is not something that would be used for incident reporting.

History Class

This class contains descriptions of the significant actions performed by the involved parties when managing the incident. The descriptions are free form, so the level of detail is left up to the involved parties. This class is optional and clearly only for incident sharing purposes, rather than for initial incident reporting.

AdditionalData Class

This class contains any extension classes that are used within the Incident class. This class is of course optional. This can be useful if any extensions are needed for the specific use case that IODEF is applied to.

After thoroughly examining the IODEF data model specification, it seems clear that all the information needed for conventional incident data reporting is representable within the model. Important things like incident ID, incident report time, contact information, incident description, and ways to add log and other files are present in the data model. Quite a lot of information specific to incident sharing can also be represented with the model. All of this is optional data, so it won't be there as a distraction when using this model for incident reporting purposes and can be added later if the incident is going to be shared outside the organization.

The use case of reporting incidents onboard an autonomous ship is certainly not the most conventional one, and some important information is currently left out of the model. The model does not consider the mobility of the target in any way. Since an autonomous ship is a moving target, positional information at the time of the incident is probably just as important as the time information itself. Identifying the vessel that is sending the incident report would also be a good idea. An extension is needed to add this kind of information to the model.

4.2 Extensions Design

An extension to the data model is needed to convey data about the vessel and the voyage. First, we need to identify all the information that needs to be included in the extension. In this case, this information includes:

- Vessel identification
- Voyage information
- Coordinates
- Speed

All this information can be provided by the AIS onboard the ship. AIS is used to monitor the movement of vessels and to control maritime traffic and it is mandatory on most vessels doing international voyages [42].

The IMO number of the vessel can be used for vessel identification, this is a number that is given to each vessel when built. This number is known for each vessel and hence easy to obtain for the data model. AIS also provides other useful identifying traits of the vessel, such as name and type. AIS includes voyage related information, such as destination and estimated time of arrival (ETA). Positional coordinates are given as degrees minutes seconds at up to 0.0001-minute accuracy for both latitude and longitude. These can be quite easily converted to decimal degrees for ease of use in the data model. Speed is given in knots with 0.1 accuracy. [43]

RFC 6684 [33] is a guideline document to designing extensions for IODEF provided by the MILE working group. The information in this document is used while designing this extension. This extension design is just a rough draft and will not be using the Internet-Draft template provided in the RFC. This extension is only for hypothetical use within this thesis but could quite easily be turned into a real extension for IODEF later.

What is needed for this extension is a completely new class containing the information that is listed earlier. This can be achieved by adding a new aggregate class for the AdditionalData class that is an aggregate class of the Incident class. Let's call this new class Shipping. A representation of this class is in Figure 7.

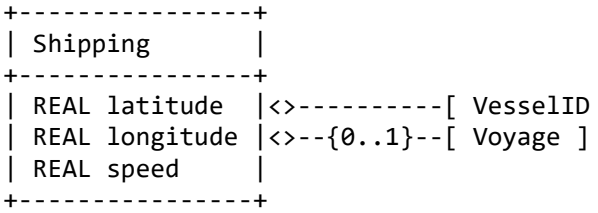

Figure 7. *A representation of the Shipping class.*

The aggregate classes of the Shipping class are:

- VesselID: Required. The IMO number assigned to this vessel. Also contains other information about the vessel.
- Voyage: Optional. Information about the voyage that the ship is on.

The attributes of the Shipping class are:

- latitude: Optional. REAL. The latitude portion of the coordinates of the vessel in decimal degree format.
- longitude: Optional. REAL. The longitude portion of the coordinates of the vessel in decimal degree format.
- speed: Optional. REAL. The current speed of the vessel in knots.

The coordinates and speed are requested at the time provided in the GenerationTime aggregate class of the Incident class. This way the information is timestamped and useful.

The VesselID class contains the IMO number, name, and type of the vessel. More identifying traits like color, size, etc. could be added to this class later on. These traits are, however, not available in the AIS so they would need to be manually configured to the model. A representation of this class is in Figure 8. The VesselID class has no aggregate classes.

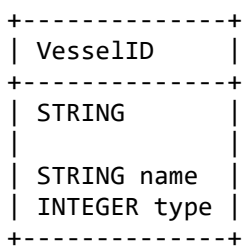

Figure 8. *A representation of the VesselID class.*

The content of this class is the IMO number of the vessel in STRING format. This information is required. IMO numbers consist of the letters “IMO” followed by seven numbers.

The attributes of the VesselID class are:

- name: Optional. STRING. The name of the vessel.
- type: Optional. INTEGER. The type of the vessel signified as a number in the AIS. List of type numbers can be found at the marine traffic website [44].

The Voyage class contains the destination and ETA of the vessel. A representation of this class is in Figure 9. The Voyage class has no aggregate classes.

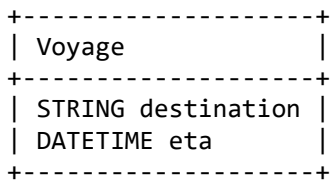

Figure 9. *A representation of the Voyage class.*

The attributes of the Voyage class are:

- destination: Optional. STRING. The name of the destination port or city of the vessel.
- eta: Optional. DATETIME. The estimated time of arrival of the vessel.

The Shipping class is required for every incident report that has anything to do with a vessel. This extension class will be tested in the example use cases in Chapter 5.

5. USE SCENARIOS AND APPLICABILITY

In this chapter, the IODEF data model is applied to couple example use scenarios. No access to full incident reports from the maritime industry was provided, so the example incidents introduced in Chapter 2.2.4 are used as example use scenarios. This means that the use scenarios are completely fictional, but still scenarios that could easily happen in real life. The example incidents are from news articles, so the information that they provide is scarce, so all the available information in these cases needs to be assumed.

These applicability tests are needed to see that the model is usable for the needs of autonomous shipping and that the model is flexible enough to be able to work in many different situations. Further testing would be needed to validate the use of this model for incident reporting on autonomous ships. These tests would include, for example, using the data model over a satellite link, inserting real life data into the data model, and testing various transmit methods. Most of these tests are, however, outside the scope of this thesis, while some additional tests are conducted in Chapter 6.

These use scenarios are introduced in the following three subchapters. Each scenario is first explained and then the available information is inserted into the data model. Some snippets of the data model XML code are given and explained, while the full IODEF-Documents for each use scenario in XML can be found in the appendices.

The first use scenario that is introduced in Chapter 5.1 gives a basic example of an incident report. Many of the most common parts of the XML schema are introduced and explained here. These parts of the schema are not explained in further scenarios to avoid redundancy. The last two scenarios in Chapters 5.2 and 5.3 bring out some more special use cases and introduce some of the less used parts of the XML schema.

5.1 Use Scenario: VDR Tampering

The example incident that will be used for this scenario is labeled as “India, 2012” in Chapter 2.2.4. In this incident, the Voyage Data Recorder (VDR) of a ship was tampered with. To bring this kind of an incident to the autonomous shipping world, let’s say that an attacker gains remote access to the VDR of the ship. This can be achieved by hacking into the systems of the ship. The goal of this kind of an attack would be to change or erase the data of the VDR.

When this kind of an attack happens, we might not at first know that the VDR is targeted. Rather, we would first notice the breach of the systems of the ship. Let's say that the breach is noticed by an Intrusion Detection System (IDS) onboard the ship. After detection, the systems would collect any available data about the incident and send the very first incident report about this incident to the shore control center. Not much is yet known about the incident, but here is the data we could assume we have at this point in time:

- Type of incident (systems breach)
- Detected by IDS
- IDS log files
- Time of the breach detection
- Location and speed of the ship at detection time

In addition to this data, there are some required fields in the data model that would still be empty. Those are incident ID, contact information, information restriction, report purpose, report generation time, and vessel ID. For the sake of this example, the data points are given values of some kind so that the data can be inserted into the model. All the information is put inside the Incident class of IODEF, which is initiated like this:

```
<Incident purpose="traceback" status="new" restriction="need-to-know">
```

The attributes of the class tell us the purpose of the incident report, its status, and the level of restriction for the information within. The incident ID is given with the IncidentID class:

```
<IncidentID name="csirt.autonomousshipping.com">123456</IncidentID>
```

The name attribute of the class specifies the incident response team that is responsible for this report. The type of the incident is signified in the Description class with the keyword "systems breach" as discussed in Chapter 4.1. This can be simply achieved like this in the model:

```
<Description>systems breach</Description>
```

The fact that the incident was detected by the IDS can be signified in the Discovery class like this:

```
<Discovery source="nidps"></Discovery>
```

Here "nidps" is a preset value for the source -attribute, defined in the IODEF specifications. It means that the discovery source was a network intrusion detection or prevention system. A link to the IDS log file location can also be added to the data model with the RecordData class:

```
<RecordData>
   <Description>IDS log file.</Description>
   <URL>systems\ids\ids.log</URL>
</RecordData>
```

The full IODEF-Document that was filled using all the aforementioned data can be found in Appendix B labeled as Report A. This is an initial incident report, and as such it is quite minimal. The report is also sent from the sea over a satellite link, so minimalism is preferred. This is what an initial report will look like in most cases.

After the initial report, the incident response team at the control center will start working on resolving the incident. The priority will be blocking the attacker from the systems of the ship. More data will be collected from the ship. With some time, the team will realize that the real target of the attack was the VDR. Further reports about the incident can be grouped under the initial breach report using the RelatedActivity class.

As the VDR was targeted it could imply that there has been some activity recorded by the VDR that the attacker wanted removed or changed, for example unauthorized access to the cargo. Another option is that the attacker was just being annoying and wanted to delete all the VDR information for no real reason. In any way, the incident should be shared with the organization that owns the cargo that the ship was carrying. Here is the information that we should share about this incident:

- Incident description
- Repercussions of the incident
- Time of the incident
- Contact information
- Ship’s IMO number

In addition to all this information, the required fields in the data model will also need to be filled again. Lots of information that doesn’t belong to the stakeholders is left out of this incident report. The specialty of this incident report lies in the fact that repercussions of the incident are given. The repercussions can be conveyed in the data model inside the Assessment class:

```
<Assessment occurence="actual">
   <IncidentCategory>VDR tampering</IncidentCategory>
   <SystemImpact
   severity="medium"
   completion="succeeded"
   type="takeover-system">
      <Description>Ship’s VDR was accessed without permission.</Description>
   </SystemImpact>
   <SystemImpact severity="high" type="integrity-data">
      <Description>VDR data was possibly altered.</Description>
   </SystemImpact>
   <BusinessImpact severity="medium" type="loss-of-integrity">
      <Description>Integrity of the VDR data was lost.</Description>
```

```
   </BusinessImpact>
   <IntendedImpact severity="medium" type="loss-of-integrity">
      <Description>
         The attacker intended to delete or change data in the VDR, causing
         loss of integrity.
      </Description>
   </IntendedImpact>
   <Cause>
      VDR tampering was made possible by a weakness in the network that has
      since been fixed.
   </Cause>
   <Confidence rating="high"></Confidence>
</Assessment>
```

Here the incident is first categorized as VDR tampering inside the IncidentCategory class. Then the impact of the incident is looked at from the system and business points of view in the SystemImpact and BusinessImpact classes. The intended impact of the attack is speculated in the IntendedImpact class. The reason why this incident could happen is given in the Cause class. Finally, a confidence rating for all this information is given in the Confidence class. The full IODEF-Document of this incident report can be found in Appendix B labeled as Report B.

5.2 Use Scenario: GPS Spoofing

This use scenario will follow the example incident labeled as “Russia, 2017” in Chapter 2.2.4. In the incident, an area at the Black Sea was targeted with GPS spoofing, causing GPS to have false signals in that area. For this use scenario, a similar situation is assumed. Let’s say that an area in front of Helsinki is targeted with GPS spoofing, causing false GPS signals in the area. GPS spoofing can be quite tricky to detect, but in this scenario, just like in the example incident, the spoofed signal “moves” the ships in the area to the shore, making it obvious that the signal is wrong. Reports of this would start flowing to the port of Helsinki pretty fast.

In this scenario, the incident report is coming from port authorities to vessels, control centers, and organizations working in the area. In the report, the situation is described, and a warning is given. This is the information that such an incident report should include:

- Description of the situation
- How the incident was detected
- Repercussions of the situation
- Method of attack
- Discovery time of the incident
- Contact for additional information

In addition to this the required fields of the model will also have to be filled. The incident is shortly described in free form within the Description class. The information on

how the incident was discovered is inside the Discovery class. The intended repercussions of the attack are assessed inside the Assessment class:

```
<Assessment occurence="actual">
   <IncidentCategory>GPS spoofing</IncidentCategory>
   <IntendedImpact severity="high" type="loss-of-service">
      <Description>
         The attack is intended to make GPS unreliable in the area.
      </Description>
   </IntendedImpact>
   <Confidence rating="high"></Confidence>
</Assessment>
```

The rating attribute inside the Confidence class is given the value “high” here to indicate that the information provided is authoritative. The confidence rating can get values low, medium and high, so the confidence level of this report is the highest possible one. The method of the attack is specified within the Method class:

```
<Method>
   <Reference>
      <Description>Link to explain GPS spoofing.</Description>
      <URL>https://en.wikipedia.org/wiki/Spoofing_attack#GPS_spoofing</URL>
   </Reference>
</Method>
```

A link to the Wikipedia article is given by the authorities as a reference for people who are not at all familiar with GPS spoofing. Contact information to the port authorities are specified within the Contact class:

```
<Contact role="creator" type="organization">
   <Description>
      Contact information to the port of Helsinki incident management team.
   </Description>
   <Email>
      <EmailTo>example@csirt.port.helsinki.fi</EmailTo>
   </Email>
   <Telephone type="hotline">
      <TelephoneNumber>+358407654321</TelephoneNumber>
   </Telephone>
</Contact>
```

Here an email address and a hotline telephone number are given. Additionally, more information about the contact person could easily be conveyed within the model as well as a postal address and time zone of the place. These are not necessary in this case. The full incident report of this scenario can be found in Appendix C.

5.3 Use Scenario: Malware

This use scenario will not follow any example incident and will be completely fictional. Let’s say that an autonomous ship is at port and its’ software is being updated. Somehow some kind of malware gets into the systems of the ship with the software update.

For this use scenario it doesn't really matter what kind of malware it is, and how it ended up in the systems of the ship.

In this scenario, the malware is quickly detected by the antivirus software of the ship and an incident report is generated and sent to the control center. What makes this scenario special, is that the ship is at port and cellular or WiFi connections are available. This means that we can send a lot more information than we could if the ship was at sea and a satellite connection was used. This extra information is not necessary but can help with the incident management. The information that we have right now includes:

- Type of incident (malware detected)
- Detected by antivirus software
- Output file from the antivirus software
- Detection time
- Ships location
- Vessel identifying traits
- Voyage information

In addition to this, all the required fields of the data model also need to be filled, as discussed in the earlier use scenarios. The type of the incident is specified with the keyword "malware detected" within the Description class. The fact that the incident was detected by antivirus software is specified with the value "av" of the source attribute of the Discovery class, this is a predetermined value for all antivirus software given in the IODEF specification. All of this is really similar to the VDR tampering use scenario in Chapter 5.1.

In this case only malware detection is reported, and the specifics can be found within the output file of the antivirus software that can be found in the RecordData class. This file should provide answers to questions such as "What was infected?", "Which malware is it?", "What caused the infection?" and many more. Confidence level of the malware detection is also displayed here. All this information is of course dependent on the antivirus software that is used.

What this use scenario was mainly designed to show is the use of the Shipping extension class. We can specify the name, type (type number 60 means passenger vessel) and IMO number of the ship in the VesselID class, and the destination and ETA of the next voyage in the Voyage class. This is how the extension would look like in this situation:

```
<AdditionalData>
   <Shipping latitude="60.161871" longitude="24.958996" speed="0">
      <VesselID name="Test Vessel II" type="60">IMO7654321</VesselID>
      <Voyage destination="Stockholm" eta="2017-12-16T22:15:00"></Voyage>
   </Shipping>
</AdditionalData>
```

Now that we have good connectivity in this use scenario, older similar incidents can be linked to the incident report to provide helpful information about how similar incidents were handled before. This can be done within the RelatedActivity class:

```
<RelatedActivity>
   <IncidentID name="csirt.autonomousshipping.com">111111</IncidentID>
   <IncidentID name="csirt.autonomousshipping.com">101010</IncidentID>
   <Confidence rating="high"></Confidence>
</RelatedActivity>
```

Here it is indicated that incidents with IDs 111111 and 101010 are related to this incident. Confidence rating “high” is given to indicate that these incidents had the same malware and can be used as reference for incident management. If we want to group together multiple incidents, for example when getting many detections from antivirus software, it can be done by adding multiple Incident classes inside the IODEF-Document class.

Other extra data that could be conveyed with the model in this situation while having good connectivity could include information about the network and systems of the ship, specific information about the malware, information about the antivirus configuration that allowed us to detect this malware, and so on. The full IODEF-Document for this use scenario can be found in Appendix D.

6. TESTING AND ANALYSIS

This chapter has further analysis and testing of the data model so that we can more confidently validate the use of the IODEF data model for the use case of autonomous shipping. Sending XML files with full incident reports over a high latency connection was tested in Chapter 6.1 to see if the connection from sea would be real-time enough. Same tests were also conducted from a more stable connection to have something to compare to.

The file sizes of IODEF-Documents are usually quite small, but the high latency introduced by having to use a satellite link connection might cause the file transfer to be somewhat slow. This problem would, however, happen with any data model as it is based on the connection, but this is still worth investigating to validate the usefulness of such an incident reporting method.

In Chapter 6.2 the data model is analyzed based on the research done. The idea is to further validate the choice of the IODEF data model through explaining why the model is good and analyzing some of the tests and work done with the model.

6.1 Transport Testing

The native point-to-point transport protocol of IODEF is RID which is also developed by the MILE working group of IETF. However, IODEF is not tied to RID and can work with any other transport protocol as well. For simplicity's sake these transport tests were conducted using SSH File Transfer Protocol (SFTP).

For these tests a laboratory network was set up at the TUT cyber security lab. The network consisted of 2 connected computers, one simulating the ship and one the shore control center. Between these computers was a link simulator that was used to change the properties of the connection. As stated earlier, the tests were conducted twice, once using a satellite link and once a cellular link. The bandwidth in megabits per second, latency in milliseconds, and packet loss ratio used to simulate these connections can be seen in Table 3. Here latency means the one-way latency between the computers.

Table 3. *The properties of the used connections.*

	Bandwidth (Mbps)	**Latency (ms)**	**Packet Loss Ratio**
4G Cellular	50	50	1%
Satellite	5	250	20%

Both connections were first tested with iperf, which is a network bandwidth measurement tool. A 2-minute run of iperf put the bandwidth of the satellite connection to 33.6 Kbps and the cellular connection to 1.15 Mbps. This means that the cellular connection has a bandwidth that is about 34 times bigger than that of the satellite connection.

Three different XML documents were created for these test transmissions containing IODEF-Documents from the test scenarios introduced in Chapter 5. The IODEF-Documents that were chosen are reports A and B from Chapter 5.1 and the report from 5.2. The report from 5.3 was not used as it had a similar file size to the one from 5.3. The file sizes of each incident report in bytes and their transport times in milliseconds can be found in Table 4.

Table 4. *The results of the transport tests.*

Incident Report	**File Size (bytes)**	**Time over 4G (ms)**	**Time over Satellite (ms)**
5.1 (A)	1347	348	3294
5.1 (B)	2831	352	4764
5.2	1847	351	2758

The transport times shown in the table are calculated from Wireshark capture files that were captured during the tests. From the capture files it can also be seen that opening the SFTP connection between the computers took under 2 seconds with the cellular connection, and considerably longer with the satellite connection. Depending on dropped packets, due to high packet loss ratio and higher latency, opening the connection could take up to 50 seconds with the satellite connection. The best-case scenario that was encountered during the tests for opening the SFTP connection over the satellite link was still over 11 seconds.

From the results it can be seen that the cellular network had such a high bandwidth that the transport times did not change at all based on the file sizes. On the satellite test, however, the transport times did change quite considerably. The Wireshark captures showed a lot of dropped packets and retransmissions on the satellite cases due to the fairly high 20% packet loss ratio. This caused most of the fluctuation in the results.

6.2 Analyzing the Data Model

In Chapter 3.2, some characteristics of a good data model were introduced. Here is how the IODEF model + extension fulfil these characteristics:

- Completeness: After the extension was added to the model, all the necessary data can now be represented with the model. This characteristic is fulfilled.

- Non-redundancy: No redundancies were found while going through the data model specification. This characteristic is fulfilled.
- Enforcement of business rules: Business rules are considered in the model, for example incident ID and contact information are required for each report. Using the same incident ID for two separate incidents is however possible without software that reads and manages the model. This characteristic is only somewhat fulfilled.
- Data reusability: If the application can read IODEF data, the data should be reusable. This characteristic is fulfilled.
- Flexibility: The model is flexible, as most data points in the model are completely optional. Only the required data for each use scenario can be represented which means no unnecessary data. The model is also extensible. This characteristic is fulfilled.
- Stability: Some real-life testing of the model would be needed to define the stability of the model. This characteristic remains to be determined.
- Elegance: This is quite a subjective metric, but in my opinion the model is quite simple and neat. However, someone new to the model might find it somewhat too complicated in some respects. This characteristic is only somewhat fulfilled.
- Communication: The model can be used to share data with various stakeholders as long as the stakeholders have software that can read IODEF data. This characteristic is fulfilled.

It seems that the model fulfils most of the characteristics of a good data model. Some of the characteristics are not fully met or are still undetermined. This isn't a problem, as fulfilling most of the points is enough, as stated in Chapter 3.2.

As stated in Chapter 3.2.1, the IODEF data model uses XML as its native format. XML is often seen as a somewhat too complicated and rigid format, that takes too much space for the information that it provides. Thankfully work is already undergoing for IODEF to use JSON format that is way more compact and can be serialized faster. This is also a huge benefit for the model in the autonomous shipping world as compact formats and faster serialization are preferred when using the slow and narrow satellite links.

Chapter 5 provides multiple use scenarios for the data model. These scenarios show that the model can be used for many different cases of incident reporting at sea. Based on these use scenarios, the data model is applicable for autonomous shipping, but more testing with real-life data would be needed to be sure. Unfortunately, no real-life data was available for this thesis work, so these tests would have to be conducted at some other time.

The use scenarios also showcase some of the more special features that the IODEF data model provides, like incident grouping, incident assessment, and of course the shipping specific class that was designed in Chapter 4.2. In addition to these, the model also has a

vast amount of other special classes that were not showcased in the use scenarios but could easily be useful in some specific incident reporting situations. This is to say that the IODEF data model really exceeds many of the other data models out there with its attention to detail and provision of data points for special use cases.

Another characteristic of the model we should take a look at is the file size of generated reports. As seen earlier, the file sizes of the reports used in the transport tests are between 1347 and 2831 bytes. The 1347-byte report is a typical first incident report, and the 2831-byte file contains a report about an incident sent to stakeholders. Reports that are sent from the ship to shore should not get much bigger than this.

The minimum file size is quite easy to determine, just fill an incident report with only the fields that are required by the model and use as short as possible values for these fields. Using this method, a file size of 635 bytes was received. This should be around the floor value of the file size. The ceiling value is a lot trickier to find, as the model includes so many optional fields and the values of these fields can vary in length. Basically, the file size can be infinite, but in practice an incident report should never get file sizes bigger than around 5000 bytes. When the model is being used to share incident information with stakeholders the file size can get bigger than that, but that use case is not as time sensitive as incident reporting, so it should not be a problem.

The hypothesis for the transport test conducted in Chapter 6.1 was that the high latency introduced by the satellite link will make the transport time considerably longer compared to the cellular network case. This is because SFTP uses Transmission Control Protocol (TCP) which has handshake packets to open the connection, and acknowledgement packets for every received data packet. The additional latency should cause the large number of packets to waste extra time.

The transport test in Chapter 6.1 showed the above hypothesis to be true. The file transfer times got around 10 times longer on average. The biggest problem however, seemed to be the connection opening, which took considerably longer on the satellite connection than on the cellular one. Based on the Wireshark captures taken during the tests, it seems that this was largely due to dropped packets that had to be retransmitted.

User Datagram Protocol (UDP) is an unreliable, connectionless, and no acknowledgements alternative to TCP. Testing of any UDP based transport protocol could be useful to see if it would be a better transmission protocol to use over a satellite link. This is, however, outside the scope of this thesis.

The transport test showed that the bandwidth of the connection doesn't really affect the transmission of these small XML files, as long as the bandwidth is at a reasonable level. Latency and packet loss ratio seem to have much more impact in this case. Based on the test it is clear that the reports won't reach the shore control center in real-time. It is not feasible to keep a connection open at all time over a satellite connection, which means

that a connection must be initiated every time a report needs to be sent, and that adds to the file transport time considerably. Even if the files won't reach the shore in real time, it is safe to assume that they get there fast enough so that incidents can be reacted to in a timely manner.

7. CONCLUSIONS

In this chapter, the thesis work is concluded by giving answers to the research questions presented in Chapter 1.1. This is done by referencing earlier chapters of the thesis and drawing conclusions from the research done there.

The first research question of the thesis is: “What is the current state of autonomous shipping?”. This was investigated in Chapter 2.1 and its subchapters. Based on this research it is safe to say that autonomous shipping is still a new and developing technology that will still need a lot of work before its widespread commercial use. It also became apparent that this work is being done right now by many different stakeholders all around the world. There are clearly still some minor and even major obstacles to cross, but these are being solved. The commercial use of autonomous shipping in some capacity is expected by the year 2025.

The second research question of the thesis is: “What is the current state of maritime physical and cyber security?”. These areas were being looked at in Chapter 2.2 and its subchapters. The maritime industry has long traditions with physical security and safety. There are clear and up-to-date guidelines and policies on physical security provided by the IMO. All in all, physical security is seen as an important thing in the industry and it is clearly in a good state right now. Cyber security is another matter, however. Maritime cyber security is a rather new branch of cyber security that has developed as ships are fitted with more and more ICT equipment. Cyber concerns were first pretty much disregarded by the industry. Nowadays the industry starts to see cyber security as more and more important, but full guidelines and policies from the IMO are still missing. The industry has come together to develop some basic guidelines for everyone to follow. All this means that the state of maritime cyber security is currently quite poor. Many improvements are needed, especially before autonomous shipping can become a widely used technology.

The third research question of the thesis is: “What are the common practices in incident management and reporting, and what kind of reporting methods are used currently?”. These areas were investigated in Chapter 3 and its subchapters. It was established that there are clear and commonly applied standards and guidelines for information security incident management. These are explained in Chapter 3 and incident reporting, that is a part of the incident management life cycle, is looked into more thoroughly in Chapter 3.1. Incident reporting and sharing methods are, however, not at all standardized and many organizations use their own methods that are tailored for the organization’s needs. Recently, as the machine-readability of incident reports and the sharing of incidents

over organization boundaries has become more important, some more standardized and commonly used methods have arisen. These include IODEF, STIX and VERIS that are introduced in Chapter 3.3.

The fourth research question of the thesis is: “What kind of a cyber security incident data reporting model would be the best for autonomous ships?”. Answers to this question were searched in Chapters 4, 5, and 6. Out of the incident reporting data models introduced in Chapter 3.3 IODEF was chosen as the best fit for this use case. This was because IODEF is flexible, extensible, has the right design philosophy, and has a near standard status. It also seemed like the most suitable one out of the three after the initial look into the models.

The IODEF specification was looked into more closely in Chapter 4.1 and an extension to the data model was designed in Chapter 4.2 to include some use case specific information that was not representable with the base model. After this addition it seems that the model would be able to represent all the needed information to report cyber security incidents from an autonomous ship to the shore control center.

The data model was then applied to different use scenarios in Chapter 5 to see if the model is applicable to this use case or not. The model was used to report incidents from an autonomous ship, to share an incident with stakeholders, and to warn ships and organizations of an ongoing attack in these use scenarios. Based on these use scenarios, the model seems applicable to reporting maritime cyber security incidents. It is also important to notice that in real-world applications the information would be displayed in a graphical user interface, making the information much more readily and easily available than trying to find the information from within the XML code.

A transport test was conducted for XML files containing IODEF-Documents in Chapter 6. This test showed that while the transport to shore can’t be called real-time, it is fast enough. The data model’s good characteristics were brought up later in Chapter 6 to further validate the use of the data model in the use case of reporting cyber security incidents from an autonomous ship.

It is important to notice that this thesis does not fully validate the use of this model, as such work is not included in the scope of this thesis. The thesis work provides a good amount of research into the IODEF data model and shows that the data model is promising. All this work will be useful later when more testing is conducted. This testing will include trying different transport methods and implementing the data model in laboratory conditions.

REFERENCES

[1] O. Levander, Forget Autonomous Cars – Autonomous Ships Are Almost Here, IEEE Spectrum, Jan 2017. Available: https://spectrum.ieee.org/transportation/marine/forget-autonomous-cars-autonomous-ships-are-almost-here

[2] G. Peters, A Decade to Autonomous Cargo Ships?, Ship Technology Global, Jul 2017. Available: http://www.ship-technology.com/features/featurea-decade-to-autonomous-cargo-ships-5838573/

[3] DIMECC Opens the First Globally Available Autonomous Maritime Test Area on the West Coast of Finland, Port News, Aug 2017. Available: http://en.portnews.ru/news/243920/

[4] The Autonomous Ship, Maritime Unmanned Navigation through Intelligence in Networks, 2016. Available: http://www.unmanned-ship.org/munin/about/the-autonomus-ship/

[5] N. Blenkey, The Nordic Influence, Marine Log, Feb 2016. Available: http://www.marinelog.com/index.php?option=com_k2&view=item&id=10534:the-nordic-influence&Itemid=231

[6] M. Lindqvist, Challenges Facing the Nordic Maritime Sector, Journal of Nordregio, No. 2, 2010. Available: http://www.nordregio.se/en/Metameny/About-Nordregio/Journal-of-Nordregio/Journal-of-Nordregio-2010/Journal-of-Nordregio-no-2-2010/Challenges-facing-the-Nordic-Maritime-Sector/

[7] K. E. Kristiansen, The Home of Disruption – Look to the Nordics for New Wave of Digital Maritime Solutions, Nor-Shipping, 2017. Available: http://nor-shipping.com/home-disruption/

[8] D. Cimpean, J. Meire, V. Bouckaert, S. V. Casteele, A. Pelle, L. Hellebooge, Analysis of Cyber Security Aspects in the Maritime Sector, European Network and Information Security Agency, Nov 2011, 31 p. Available: https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1/at_download/fullReport

[9] L. Jensen, Challenges in Maritime Cyber-Resilience, Technology Innovation Management Review, Vol. 5, Iss. 4, Apr 2015, pp. 35–39. Available: https://search.proquest.com/docview/1676101493?pq-origsite=gscholar

[10] S. Ahvenjärvi, The Human Element and Autonomous Shipping, TransNav: International Journal on Marine Navigation and Safety of Sea Transportation, Vol. 10, No. 3, Gdynia Maritime University, Sep 2016, pp. 517–521. Available: https://doaj.org/article/c4104d7e5f874264b34bd720b4b380a5

[11] B. M. Batalden, P. Leikanger, P. Wide, Towards Autonomous Maritime Operations, 2017 IEEE International Conference on Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA), Annecy, 2017, 6 p. Available: http://ieeexplore.ieee.org/document/7995339/

[12] D8.6: Final Report: Autonomous Bridge, Maritime Unmanned Navigation through Intelligence in Networks, Aug 2015, 17 p. Available: http://www.unmanned-ship.org/munin/wp-content/uploads/2015/09/MUNIN-D8-6-Final-Report-Autonomous-Bridge-CML-final.pdf

[13] F. Cassidy, NMEA 2000 Explained – The Latest Word, NMEA Standards Committee, Mar 1999, 17 p. Available: https://www.nmea.org/Assets/2000-explained-white-paper.pdf

[14] T. Hogg, S. Ghosh, Autonomous Merchant Vessels: Examination of Factors That Impact the Effective Implementation of Unmanned Ships, Australian Journal of Maritime and Ocean Affairs, Vol. 8, Iss. 3, 2016, pp. 206–222. Available: https://search.proquest.com/docview/1858080492?pq-origsite=summon

[15] IMO Maritime Security Measures – Background, Maritime Security Section International Maritime Organization, Jan 2008, 12 p. Available: http://www.osce.org/eea/30455?download=true

[16] MSC-FAL.1/Circ.3: Guidelines on Maritime Cyber Risk Management, International Maritime Organization, Jul 2017, 6 p. Available: http://www.segumar.com/wp-content/uploads/2017/08/MSC-FAL.1-Circ.3.pdf

[17] BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF, IUMI, The Guidelines on Cyber Security Onboard Ships, Ver. 2.0, 2017, 51 p. Available: http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=14

[18] S. Parkinson, P. Ward, K. Wilson, J. Miller, Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges, IEEE Transactions on Intelligence

Transportation Systems, Vol. 18, No. 11, Nov 2017, pp. 2898–2915. Available: http://ieeexplore.ieee.org/abstract/document/7872388/

[19] T. Bateman, Police Warning After Drug Traffickers' Cyber-Attack, BBC News, Oct 2013. Available: http://www.bbc.com/news/world-europe-24539417

[20] J. Saul, Global Shipping Feels Fallout from Maersk Cyber Attack, Reuters, Jun 2017. Available: https://www.reuters.com/article/us-cyber-attack-maersk/global-shipping-feels-fallout-from-maersk-cyber-attack-idUSKBN19K2LE

[21] R. Santamarta, Maritime Security: Hacking into a Voyage Data Recorder (VDR), IOActive, Dec 2015. Available: http://blog.ioactive.com/2015/12/maritime-security-hacking-into-voyage.html

[22] S. J. Freedberg Jr., Was the Merchant Ship Hacked? McCain Collision Is First Run for Navy Cyber Investigators, Breaking Defense, Sep 2017. Available: https://breakingdefense.com/2017/09/mccain-collision-is-dry-run-for-navy-cyber-investigators/

[23] D. Hambling, Ships Fooled in GPS Spoofing Attack Suggest Russian Cyberweapon, New Scientist, Aug 2017. Available: https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/

[24] ISO/IEC 27035-1:2016 Preview, International Organization for Standardization, Nov 2016. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27035:-1:ed-1:v1:en

[25] P. Cichonski, T. Millar, T. Grance, K. Scarfone, NIST Special Publication 800-61: Computer Security Incident Handling Guide, Revision 2, National Institute of Standards and Technology, Aug 2012, 79 p. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[26] I. A. Tøndel, M. B. Line, M. G. Jaatun, Information Security Incident Management: Current Practice as Reported in the Literature, Computers & Security, Vol. 45, Sep 2014, pp. 42–57. Available: http://www.sciencedirect.com/science/article/pii/S0167404814000819

[27] E. Koivunen, "Why Wasn't I Notified?": Information Security Incident Reporting Demystified, Information Security Technology for Applications, NordSec 2010, Lecture Notes in Computer Science, Vol. 7127, 2012, pp. 55–70. Available: https://link.springer.com/chapter/10.1007/978-3-642-27937-9_5

[28] G. C. Simsion, G. C. Witt, Data Modeling Essentials, Third Edition, 2005, 531 p. Available:

https://books.google.fi/books?id=0f9oLxovqIMC&printsec=frontcover#v=onepage&q&f=false

[29] Charter for Working Group, MILE Working Group, 2016. Available: https://datatracker.ietf.org/wg/mile/about/

[30] Managed Incident Lightweight Exchange (MILE) Working Group Overview, IETF, 2013. Available: https://trac.ietf.org/trac/mile

[31] R. Danyliw, RFC 7970: The Incident Object Description Exchange Format Version 2, IETF, Nov 2016, 172 p. Available: https://tools.ietf.org/html/rfc7970

[32] T. Takahashi, M. Suzuki, JSON Binding for IODEF, MILE Working Group, Sep 2017, 60 p. Available: https://tools.ietf.org/html/draft-ietf-mile-jsoniodef-00

[33] B. Trammell, RFC 6684: Guidelines and Template for Defining Extensions to the Incident Object Description Exchange Format (IODEF), IETF, Jul 2012, 12 p. Available: https://tools.ietf.org/html/rfc6684

[34] K. Moriarty, RFC 6545: Real-time Inter-network Defense (RID), IETF, Apr 2012, 84 p. Available: https://tools.ietf.org/html/rfc6545

[35] J. Field Pivotal, S. Banghart, D. Waltermire, Resource-Oriented Lightweight Information Exchange, MILE Working Group, Sep 2017, 46 p. Available: https://tools.ietf.org/html/draft-ietf-mile-rolie-10

[36] Sharing Threat Intelligence Just Got a Lot Easier!, OASIS Cyber Threat Intelligence Technical Committee, 2017. Available: https://oasis-open.github.io/cti-documentation/

[37] B. Jordan, R. Piazza, J. Wunder, STIX Version 2.0. Part 1: STIX Core Concepts, OASIS Cyber Threat Intelligence Technical Committee, Jun 2017, 68 p. Available: https://docs.google.com/document/d/1dIrh1Lp3KAjEMm8o2VzAmuV0Peujt9aAh1IHrjAroM/pub

[38] Introduction to STIX, OASIS Cyber Threat Intelligence Technical Committee, 2017. Available: https://oasis-open.github.io/cti-documentation/stix/intro

[39] B. Jordan, R. Piazza, J. Wunder, STIX Version 2.0. Part 2: STIX Objects, OASIS Cyber Threat Intelligence Technical Committee, Jun 2017, 58 p. Available: https://docs.google.com/document/d/1IvkLxg_tCnICsatu2lyxKmWmh1gY2h8HUNssKIE-UIA/pub

[40] Introduction to TAXII, OASIS Cyber Threat Intelligence Technical Committee, 2017. Available: https://oasis-open.github.io/cti-documentation/taxii/intro

[41] The Vocabulary for Event Recording and Incident Sharing (VERIS), VERIS Community, 2017. Available: http://veriscommunity.net/index.html

[42] What Is the Automatic Identification System (AIS)?, Marine Traffic Help, 2017. Available: https://help.marinetraffic.com/hc/en-us/articles/204581828-What-is-the-Automatic-Identification-System-AIS-

[43] What Kind of Information Is AIS-Transmitted?, Marine Traffic Help, 2017. Available: https://help.marinetraffic.com/hc/en-us/articles/205426887-What-kind-of-information-is-AIS-transmitted-

[44] What Is the Significance of the AIS Shiptype Number?, Marine Traffic Help, 2017. Available: https://help.marinetraffic.com/hc/en-us/articles/205579997

APPENDIX A: A LIST OF POSSIBLY VULNERABLE EQUIPMENT IN THE SYSTEMS OF A SHIP

This list is mostly taken from "The Guidelines on Cyber Security Onboard Ships" [17] but is modified to only include equipment that would be on an autonomous ship. This means that equipment that is concerned with crew or passengers is removed from the list.

Communication systems

- integrated communication systems
- satellite communication equipment
- wireless networks (WLANs)
- public address and general alarm systems

Bridge systems

- integrated navigation system
- positioning systems (GPS, etc.)
- Electronic Chart Display Information System (ECDIS)
- Dynamic Positioning (DP) systems
- systems that interface with electronic navigation systems and propulsion/maneuvering systems
- Automatic Identification System (AIS)
- Global Maritime Distress and Safety System (GMDSS)
- radar equipment
- Voyage Data Recorders (VDRs)
- other monitoring and data collection systems

Propulsion and machinery management and power control systems

- engine governor
- power management
- integrated control system
- alarm system
- emergency response system

Access control systems

- surveillance systems such as CCTV network
- Bridge Navigational Watch Alarm System (BNWAS)
- Shipboard Security Alarm Systems (SSAS)

Cargo management systems

- Cargo Control Room (CCR) and its equipment
- level indication system
- valve remote control system
- ballast water systems
- water ingress alarm system

Core infrastructure systems

- security gateways
- routers
- switches
- firewalls
- Virtual Private Network(s) (VPN)
- Virtual LAN(s) (VLAN)
- intrusion prevention systems
- security event logging systems

APPENDIX B: THE FULL IODEF-DOCUMENTS FOR THE USE SCENARIO IN CHAPTER 5.1

Report A:

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Initial incident report -->
<IODEF-Document
version="2.00"
xml:lang="en"
xmlns="urn:ietf:params:xml:ns:iodef-2.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.iana.org/assignments/xml-
registry/schema/iodef-2.0.xsd">
   <Incident purpose="traceback" status="new" restriction="need-to-know">
      <IncidentID name="csirt.autonomousshipping.com">123456</IncidentID>
      <DetectTime>2017-11-08T07:11:42</DetectTime>
      <GenerationTime>2017-11-08T07:12:16</GenerationTime>
      <Description>systems breach</Description>
      <Discovery source="nidps"></Discovery>
      <Contact role="creator" type="organization">
         <Description>
            Contact information to the organization’s CSIRT.
         </Description>
         <Email>
            <EmailTo>example@csirt.autonomousshipping.com</EmailTo>
         </Email>
         <Telephone type="hotline">
            <TelephoneNumber>+358401234567</TelephoneNumber>
         </Telephone>
      </Contact>
      <EventData>
         <Record>
            <RecordData>
               <Description>IDS log file.</Description>
               <URL>systems\ids\ids.log</URL>
            </RecordData>
         </Record>
      </EventData>
      <AdditionalData>
         <Shipping latitude="59.654041" longitude="19.846802" speed="23.7">
            <VesselID>IMO1234567</VesselID>
         </Shipping>
      </AdditionalData>
   </Incident>
</IODEF-Document>
```

Report B:

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Sharing the incident with stakeholders -->
<IODEF-Document
version="2.00"
xml:lang="en"
xmlns="urn:ietf:params:xml:ns:iodef-2.0"
```

```
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.iana.org/assignments/xml-
registry/schema/iodef-2.0.xsd">
   <Incident purpose="reporting" status="resolved" restriction="partner">
      <IncidentID name="csirt.autonomousshipping.com">123456</IncidentID>
      <DetectTime>2017-11-08T07:11:42</DetectTime>
      <GenerationTime>2017-12-04T15:11:47</GenerationTime>
      <Description>
         The ship’s voyage data recorder was accessed maliciously by an
         unknown attacker. Some data in the VDR might have been changed. This
         would indicate that something has happened to the ship at some point
         that the attacker wants to conceal. Please check your cargo for any
         anomalies when it arrives. Feel free to contact our incident
         management team with any questions you might have. Contact
         information is provided in this incident report.
      </Description>
      <Assessment occurence="actual">
         <IncidentCategory>VDR tampering</IncidentCategory>
         <SystemImpact
         severity="medium"
         completion="succeeded"
         type="takeover-system">
            <Description>
               Ship’s VDR was accessed without permission.
            </Description>
         </SystemImpact>
         <SystemImpact severity="high" type="integrity-data">
            <Description>VDR data was possibly altered.</Description>
         </SystemImpact>
         <BusinessImpact severity="medium" type="loss-of-integrity">
            <Description>Integrity of the VDR data was lost.</Description>
         </BusinessImpact>
         <IntendedImpact severity="medium" type="loss-of-integrity">
            <Description>
               The attacker intended to delete or change data in the VDR,
               causing loss of integrity.
            </Description>
         </IntendedImpact>
         <Cause>
            VDR tampering was made possible by a weakness in the network,
            that has since been fixed.
         </Cause>
         <Confidence rating="high"></Confidence>
      </Assessment>
      <Contact role="reporter" type="organization">
         <Description>
            Contact information to the organization’s CSIRT.
         </Description>
         <Email>
            <EmailTo>example@csirt.autonomousshipping.com</EmailTo>
         </Email>
         <Telephone type="hotline">
            <TelephoneNumber>+358401234567</TelephoneNumber>
         </Telephone>
      </Contact>
      <Contact role="admin" type="person">
         <ContactName>Ezekiel Example</ContactName>
         <Description>
            Contact information to the organization’s administrator.
```

```
         </Description>
         <Email>
            <EmailTo>ezekiel.example@autonomousshipping.com</EmailTo>
         </Email>
         <Telephone type="mobile">
            <TelephoneNumber>+358407654321</TelephoneNumber>
         </Telephone>
      </Contact>
      <AdditionalData>
         <Shipping>
            <VesselID>IMO1234567</VesselID>
         </Shipping>
      </AdditionalData>
   </Incident>
</IODEF-Document>
```

APPENDIX C: THE FULL IODEF-DOCUMENT FOR THE USE SCENARIO IN CHAPTER 5.2

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- GPS spoofing warning report -->
<IODEF-Document
version="2.00"
xml:lang="en"
xmlns="urn:ietf:params:xml:ns:iodef-2.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.iana.org/assignments/xml-
registry/schema/iodef-2.0.xsd">
   <Incident purpose="watch" status="new" restriction="public">
      <IncidentID name="csirt.port.helsinki.fi">654321</IncidentID>
      <DetectTime>2017-12-05T11:52:53</DetectTime>
      <GenerationTime>2017-12-05T12:04:33</GenerationTime>
      <Description>
         False GPS signals have been detected at sea in front of Helsinki.
         GPS spoofing suspected. Be mindful of   this when sailing in the
         area. This warning has been issued to all vessels and maritime
         organizations in the area.
      </Description>
      <Discovery source="external-notification">
         <Description>
            The incident was reported to port from multiple vessel at the
            area.
         </Description>
      </Discovery>
      <Assessment occurence="actual">
         <IncidentCategory>GPS spoofing</IncidentCategory>
         <IntendedImpact severity="high" type="loss-of-service">
            <Description>
               The attack is intended to make GPS unreliable in the area.
            </Description>
         </IntendedImpact>
         <Confidence rating="high"></Confidence>
      </Assessment>
      <Method>
         <Reference>
            <Description>Link to explain GPS spoofing.</Description>
            <URL>
               https://en.wikipedia.org/wiki/Spoofing_attack#GPS_spoofing
            </URL>
         </Reference>
      </Method>
      <Contact role="creator" type="organization">
         <Description>
            Contact information to the port of Helsinki incident management
            team.
         </Description>
         <Email>
            <EmailTo>example@csirt.port.helsinki.fi</EmailTo>
         </Email>
         <Telephone type="hotline">
            <TelephoneNumber>+358407654321</TelephoneNumber>
         </Telephone>
```

```
      </Contact>
   </Incident>
</IODEF-Document>
```

APPENDIX D: THE FULL IODEF-DOCUMENT FOR THE USE SCENARIO IN CHAPTER 5.3

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Malware incident report -->
<IODEF-Document
version="2.00"
xml:lang="en"
xmlns="urn:ietf:params:xml:ns:iodef-2.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.iana.org/assignments/xml-
registry/schema/iodef-2.0.xsd">
   <Incident purpose="traceback" status="new" restriction="need-to-know">
      <IncidentID name="csirt.autonomousshipping.com">123123</IncidentID>
      <DetectTime>2017-12-15T14:33:12</DetectTime>
      <GenerationTime>2017-12-15T14:35:55</GenerationTime>
      <ReportTime>2017-12-15T14:36:03</ReportTime>
      <Description>malware detected</Description>
      <Discovery source="av"></Discovery>
      <RelatedActivity>
         <IncidentID name="csirt.autonomousshipping.com">111111</IncidentID>
         <IncidentID name="csirt.autonomousshipping.com">101010</IncidentID>
         <Confidence rating="high"></Confidence>
      </RelatedActivity>
      <Contact role="creator" type="organization">
         <Description>
            Contact information to the organization’s CSIRT.
         </Description>
         <Email>
            <EmailTo>example@csirt.autonomousshipping.com</EmailTo>
         </Email>
         <Telephone type="hotline">
            <TelephoneNumber>+358401234567</TelephoneNumber>
         </Telephone>
      </Contact>
      <EventData>
         <Record>
            <RecordData>
               <Description>Antivirus software output file.</Description>
               <URL>systems\av\2017_12_15.log</URL>
            </RecordData>
         </Record>
      </EventData>
      <AdditionalData>
         <Shipping latitude="60.161871" longitude="24.958996" speed="0">
            <VesselID name="Test Vessel II" type="60">IMO7654321</VesselID>
            <Voyage
            destination="Stockholm"
            eta="2017-12-16T22:15:00">
            </Voyage>
         </Shipping>
      </AdditionalData>
   </Incident>
</IODEF-Document>
```